DISEÑO E IMPLEMENTACIÓN DE UNA APLICACIÓN WEB ORIENTADA A GENERAR CONCIENCIA Y CULTURA SOBRE LA SEGURIDAD DE LA INFORMACIÓN

GERMÁN DARÍO BELTRÁN CONSTAÍN
DIEGO FERNANDO MOSQUERA BETANCOURT

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

DISEÑO E IMPLEMENTACIÓN DE UNA APLICACIÓN WEB ORIENTADA A GENERAR CONCIENCIA Y CULTURA SOBRE LA SEGURIDAD DE LA INFORMACIÓN

GERMÁN DARÍO BELTRÁN CONSTAÍN
DIEGO FERNANDO MOSQUERA BETANCOURT

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR AL TÍTULO DE:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTORA:
LORENA OCAMPO CORREA
INGENIERA DE SISTEMAS Y COMPUTACIÓN - ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

Nota de aceptación:

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D. C. 12 de julio de 2016

A nuestras familias por su apoyo incondicional.

AGRADECIMIENTOS

Un sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización del presente trabajo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE GRÁFICOS

pág.

GLOSARIO

ACTIVO: Cualquier cosa que tenga valor para la organización. [1]

ACEPTACIÓN DEL RIESGO: Decisión informada de asumir un riesgo concreto [2]

AMENAZA: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización. [3]

ANÁLISIS DEL RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [4]

BASE DE DATOS: Entidad que almacena información de manera estructurada, generalmente sobre el usuario y/o la red. [5]

CONCIENCIA: Conocimiento reflexivo de las cosas.[6]

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [7]

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. [8]

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [9]

---

[1] Norma ISO/IEC 27000:2014
[2] Norma ISO/IEC 27000:2014
[3] Norma ISO/IEC 27000:2014
[4] Norma ISO/IEC 27000:2014
[5] Unión Internacional de Telecomunicaciones – ITU, 1998
[6] REAL ACADEMIA DE LA LENGUA ESPAÑOLA. 2015
[7] Norma ISO/IEC 27000:2014
[8] Norma ISO/IEC 27000:2014
[9] Norma ISO/IEC 27000:2014

EVENTOS EN SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad.[10]

FRAMEWORK: define un conjunto de interfaces de programación de aplicaciones (API) y de clases para el desarrollo de aplicaciones y servicios para proporcional al sistema o desarrollo de aplicaciones. [11]

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos. .[12]

GAMIFICACIÓN: El término procede de “Game”, juego en inglés, de éste se construye el neologismo “Gamificación”. Consiste en el uso del enfoque y elementos del diseño de los videojuegos en contextos diferentes al juego, con .el objetivo de hacer más atractivos interesantes las experiencias en procesos, proyectos, entre otros.[13]

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud. [14]

PHISHING: Un intento generalmente criminal de adquirir información o datos sensibles fraudulentamente, como nombres de usuario, contraseñas y detalles de cuentas financieras, haciéndose pasar por una entidad de confianza en una comunicación electrónica. [15]

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo o grupos de activos de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [16]

---

[10] Norma ISO/IEC 27000:2014
[11] Unión Internacional de Telecomunicaciones – ITU, 2011
[12] Norma ISO/IEC 27000:2014
[13] VALERA MARISCAL Juan J. F. Gamificación en la Empresa. Madrid: Editorial Círculo Rojo, 2013. Pág 30.
[14] Norma ISO/IEC 27000:2014
[15] Unión Internacional de Telecomunicaciones – ITU, 2008
[16] Norma ISO/IEC 27000:2014

SOA: Arquitectura Orientada a Servicios (SOA), siglas del inglés Service Oriented Architecture. Se refiere a la arquitectura de un sistema de información diseñado en torno a los servicios que implementan los procesos de negocio. En comparación con una arquitectura distribuida tradicional, la arquitectura orientada a servicios se distingue por su énfasis en la mutabilidad. [17]

USUARIO: Persona, organización o sistema de telecomunicaciones que tiene acceso a la red para comunicarse a través de los servicios prestados por ésta. [18]

VULNERABILIDAD: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. [19]

[17] Unión Internacional de Telecomunicaciones – ITU, 2013
[18] Unión Internacional de Telecomunicaciones – ITU, 2001
[19] Norma ISO/IEC 27000:2014

RESUMEN

Al realizar un análisis sobre los diferentes componentes del proceso de implementación de una seguridad de la información gestionable y con un ciclo de mejora continua, una de las muchas conclusiones, pero fundamental, es que uno de los factores de éxito más importantes es la concienciación del talento humano.

Teniendo en cuenta lo antes mencionado, en busca de una solución eficaz, se diseña e implementa una aplicación web que permite mediante conceptos actuales de “gamificación” hacer una difusión de seguridad de la información personalizada al interior de una organización.

Palabras clave: Sensibilización, Gamificación, Seguridad de la Información, Gestión de Seguridad de la Información, Herramienta Web.

INTRODUCCIÓN

El ser humano a través de sus acciones se convierte en un factor relevante en el mundo de la seguridad de la información. A medida que el hombre ha requerido indagar en la información resultante de sus actividades, le ha otorgado valor de acuerdo con la utilidad que le aporta a sus procesos; de ésta manera, nace la necesidad de protegerla en todos los entornos en los cuales sea generada y utilizada. El aseguramiento de los datos, que son la base de la información que nutre las actividades de las organizaciones, motiva la implementación de los Sistemas de Gestión de la Seguridad de la Información, para lo cual se requiere la vinculación activa de todo el recurso humano, quien es el responsable del uso de la información y las consecuencias del mismo. Por ello, deberá ser instruido en el uso adecuado de las herramientas tecnológicas de gestión de la información, políticas y procedimientos que garanticen la seguridad de la información. Dicho proceso formativo llevará a la generación de entornos seguros y una cultura orientada a la protección de la información.

En Colombia, el gobierno nacional dentro del marco de implementación de la estrategia de gobierno en línea, en su fase 4, define las diferentes actividades para la implementación del modelo de seguridad de la información para sensibilizar a las entidades tanto públicas y privadas como al ciudadano colombiano en la utilización y provecho del modelo de seguridad de la información.
Para la realización de la fase de sensibilización, dicha estrategia sugiere que la divulgación y sensibilización en seguridad de la información se realice a través del uso de los siguientes medios:

- Medios impresos: Afiches, brochures y elementos de recordación que contendrán información resumida pero importante acerca del modelo de seguridad de la información, en qué consiste, cuáles son sus objetivos principales y cuál es la responsabilidad de las entidades, funcionarios y empleados dentro del modelo de seguridad.

- Medios interactivos: Fondos de escritorio para los computadores de las entidades, salva pantallas, videos, con información relacionada a las principales políticas en seguridad de la información.

- A través de Internet: Presentación de información completa y detallada en la Intranet Gubernamental de Gobierno en Línea, documentos de trabajo, diagramación de procesos y servicios relacionados con el Modelo de seguridad.

En el presente trabajo de grado se encontrará el desarrollo de una alternativa, basada en medios interactivos por medio del uso de herramientas web, que brinda a las entidades de naturaleza pública o privada la posibilidad de sensibilizar y promover la seguridad de la información en la organización.

En primer lugar, se estudia la tendencia en cuanto a métodos de aprendizaje, la cual será articulada en el desarrollo de la herramienta web planteada en el presente trabajo de grado, posteriormente, se realiza el análisis de requerimientos funcionales y no funcionales, identificando además, los casos de uso y de abuso según la metodología de desarrollo seguro. Luego, se realiza la respectiva comparación de los frameworks de desarrollo Web que soportan dichos requerimientos, para luego evaluar y escoger la herramienta adecuada y finalmente, se presenta el diseño de la herramienta, el diagrama de la arquitectura de la herramienta al igual que el resultado funcional.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Implementar una aplicación web que esté orientada a generar conciencia y cultura sobre la seguridad de la información para usuarios finales.

1.2 OBJETIVOS ESPECÍFICOS

Diseñar una aplicación identificando los requerimientos funcionales estructurando la lógica del sistema e incluyendo el diseño de la interfaz gráfica de usuario.

Generar el contenido de la aplicación basado en estándares internacionales, recomendaciones, buenas prácticas y casos reales o noticias que estén orientadas a generar impacto en el usuario, para adquirir compromiso, conciencia y cultura con la seguridad de la información.

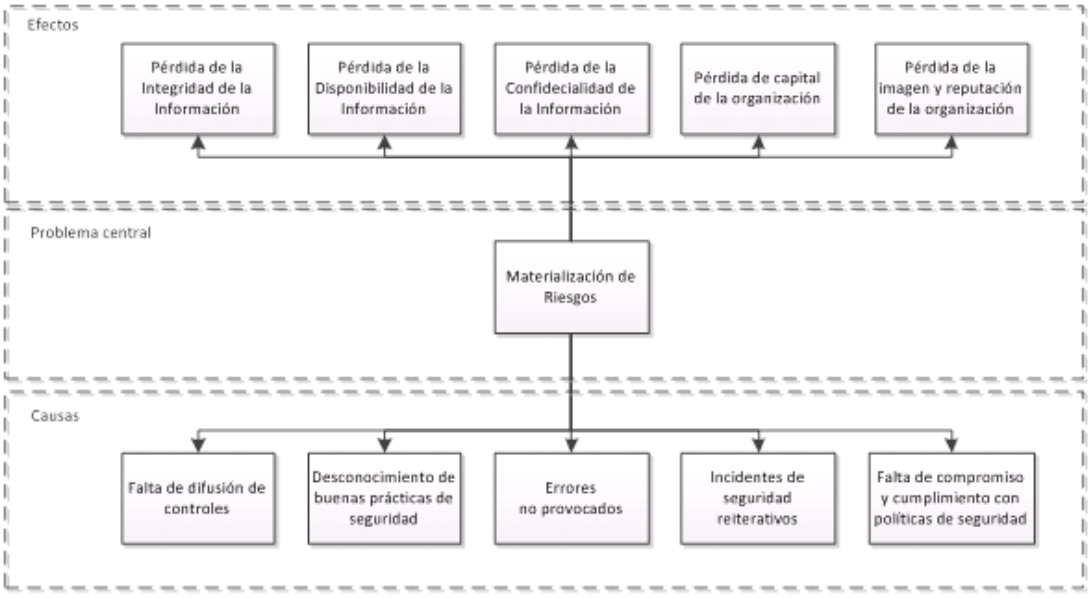
Construir un prototipo de la aplicación diseñada que se ejecute sobre un entorno WEB.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

En la actualidad las organizaciones invierten cantidades significativas de dinero en controles que garanticen la integridad, disponibilidad y confidencialidad de la información, en una gran medida, las organizaciones invierten su capital en sistemas de gestión, equipos de seguridad perimetral, centros de administración, respuesta a incidentes, control de cambios y manejo de autenticación, entre otras. Sin embargo, realizan una inversión menor en estrategias de comunicación que logren que los miembros que integran la organización se comprometan con todos los aspectos relacionados a la seguridad de la información, estrategias de comunicación que logren crear una cultura alrededor de la integridad, confidencialidad e integridad de la información, lograr un entendimiento en la organización de la importancia de salvaguardar la información. Igualmente una sensibilización exitosa debe lograr concientizar a las personas de los riesgos en su entorno, que pueden afectarlos o afectar los objetivos estratégicos de la organización, su capital, imagen, reputación o activos de información, tal como se observa en el árbol de problemas de la Figura 1. Árbol de problemas.

Figura 1. Árbol de problemas



Fuente: Elaboración propia.

2.2 JUSTIFICACIÓN

En el entorno de la seguridad de la información, siempre se busca garantizar altos niveles de protección para la información, meta ideal que requiere sumar grandes esfuerzos tanto en recurso humano como en infraestructura tecnológica. En muchas ocasiones los esfuerzos en seguridad de la información son vistos por los usuarios finales y la gente del común como barreras que dificultan la apropiación y uso de las Tecnologías de la Información y las Comunicaciones (TIC), ya que en cierto modo restringen y limitan las actividades que pueden ser desarrolladas con ellas y los resultados esperados.

En la actualidad el acceso a las tecnologías de información se ha masificado, brindando con ello una serie de entornos que han facilitado el desarrollo de las actividades cotidianas; a su vez la gran acogida que ha tenido el desarrollo tecnológico abre las puertas a un gran cúmulo de conocimiento e información, la cual puede o no ser verdadera y exacta. Del uso que se dé a dicha información dependen los efectos que se generen, los cuales pueden afectar positiva o negativamente al usuario, la comunidad, las empresas y en general a su entorno. Dicho de otra manera, el ser humano es responsable del uso que hace de la información y las consecuencias que esto genera. La falta de conciencia en el manejo y uso de la información individual o colectiva, conlleva a que se presenten incidentes de seguridad y posibles hechos delictivos que pueden afectar directa o indirectamente los intereses particulares, empresariales y de la vida cotidiana. Por ende, motivar el uso consiente y racional de la información en todas sus presentaciones, disminuirá la capacidad de que agentes externos puedan permear la privacidad de las personas y su entorno.

En todo momento el ser humano tiene a su alcance información de diversos orígenes como son académicos, laborales, públicos, entre otros; de acuerdo con la valoración que se le otorgue a la misma, ésta debe ser resguardada. Éste proceso de salvaguarda de la información va encaminado en los ámbitos empresariales y corporativos a la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual busca garantizar la protección de los activos de información que en determinadas circunstancias pueden ser los más valiosos para la organización

El ser humano por su naturaleza y carácter social es en esencia influenciable en mayor o menor proporción. Éste factor convierte al hombre en “el eslabón más débil en la cadena” de la seguridad de la información, no obstante él también interviene

de manera activa y permanente en los procesos que nacen de las áreas o departamentos encargados de las Tecnologías de la Información (TI) que están orientados a garantizar y conservar la seguridad de la información.

Dentro de la gestión de riesgo uno de los factores importantes a tener en cuenta es el ser humano, donde éste requiere conocimiento, conciencia y compromiso en la seguridad de la información, para que el desarrollo de sus actividades este acorde a la aplicación de buenas prácticas que contribuyan a tener un entorno de trabajo seguro en el desarrollo de las actividades de sus procesos. Actualmente existe una gran cantidad de controles y herramientas que contribuyen a mitigar o eliminar riesgos técnicos y de gestión, sin embargo el campo académico no ha mostrado un avance tan contundente como en los dos casos anteriores, es por eso que el presente trabajo de grado se ha orientado al eslabón más débil en la cadena de la seguridad de la información en análisis de riesgos. Es importante resaltar que en el presente trabajo de grado al igual que en varios artículos científicos, se considera que una de las vulnerabilidades más grandes en la gestión de la seguridad de la información es el usuario final, lo que no quiere decir que todas las incidencias en seguridad que se producen en una organización son culpa del usuario, pero si puede significar que el usuario no suele estar consciente de las posibles amenazas existentes o el riesgo que supone para los activos de la organización un mal uso de sus herramientas de trabajo.

Por lo anterior, se deben definir los lineamientos que se han de tener en cuenta al momento de cuidarla y conservarla para mantener vigentes sus atributos más importantes como son: la confidencialidad, la integridad y la disponibilidad. El ser humano, es quien necesita de la información para poder realizar sus tareas, alcanzar sus metas, ser competitivo y tener éxito, por ello es el directo responsable de su cuidado y conservación, para ello debe estar preparado.

Ante el auge tecnológico y el gran valor que adquiere la información como activo primordial de las organizaciones y del hombre, se debe iniciar el fomento de una Cultura de la Seguridad de la Información, que no es más que unir esfuerzos encaminados a la formación integral del ser humano para lograr su correcto desarrollo y desenvolvimiento en todos los aspectos y escenarios de la vida (personal, académico, laboral, social, cultural, entre otros); para esto se debe tener en cuenta la fundamentación en los principios éticos y morales, que le permitan discernir claramente entre lo bueno y lo malo en su entorno cotidiano.

Nuevas técnicas como el Phishing o la ingeniería social (que consiste en obtener información confidencial a través de la manipulación de usuarios legítimos), son algunas de las amenazas que están usando los piratas informáticos para acceder a la información de personas y empresas. Así mismo hay que tener en cuenta que existen otras formas fáciles de obtener datos sin conocer cuál será el uso de los mismos como por ejemplo la aplicación de encuestas, el diligenciamiento de formularios en entidades públicas o privadas, el registro que se realiza a la entrada de algún edificio o cuando se ingresa a una página web.[20]

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. De acuerdo con el estudio de ciberdelito desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), el Phishing o robo de datos personales significa pérdidas anuales por unos US$93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región, en tanto los robos a cuentas de clientes suman otros US$761 millones de dólares. Asimismo, según cifras del estudio de McAfee Inc. y Science Applications International Corporation, 25% de las organizaciones han sufrido la paralización o atraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos[21].

Cabe mencionar que empresas e instituciones de todo el mundo gastaron 338 mil millones de dólares en 2011, para combatir ataques cibercriminales, dos tercios de los cuales fueron delitos de fraude económico, de acuerdo con números ofrecidos durante el Programa de Ciberseguridad y Cibercrimen de la ONU.

Dadas las anteriores situaciones, en Colombia el Gobierno Nacional expidió el 17 de octubre de 2012, la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales. En ella se regula

[20] PORTAFOLIO. Seguridad Informática Certicámara S.A. [Citado el 02 de Abril de 2016] Disponible en http://blogs.portafolio.co/seguridad-informatica-certicamara-sa/proteccion-de-datos-personales-una-cultura-de-seguridad/

[21] PORTAFOLIO. Pérdidas delitos informáticos, [Citado el 02 de Abril de 2016] Disponible en http://www.portafolio.co/economia/finanzas/perdidas-delitos-informaticos-suman-us-93-000-millones-91548

el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”, la cual se divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

Teniendo en cuenta lo anterior, se resalta la importancia de las campañas de sensibilización y capacitaciones que las organizaciones puedan ofrecer a sus funcionarios, contratistas e inclusive proveedores sobre los riesgos, las normas y leyes vigentes, las políticas internas, las buenas prácticas en seguridad de la información, entre muchos otros.

Al observar como actualmente se manejan campañas de sensibilización en seguridad de la información, bien sea en entornos laborales o comerciales, se puede ver como, por ejemplo en un entorno laboral, la campaña está basada en salvapantallas y volantes con información que las personas no leen, no entienden o no le dan importancia e incluso en algunos casos son entendidas como una carga laboral adicional a las funciones que se vienen realizando. En casos comerciales como por ejemplo en la relación banco – cliente, se suelen utilizar campañas basadas en correos electrónicos y clausulas legales que descargan la responsabilidad de la organización al entregar y hacer aceptar al usuario una serie de cláusulas en documento de gran extensión con letra pequeña prácticamente ilegible.

Es por lo anterior que buscar alternativas efectivas para capacitar y sensibilizar a las partes interesadas es de gran utilidad.

3. MARCO TEÓRICO

3.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Las organizaciones de cualquier tipo y tamaño (incluido el sector público y privado, comercial y sin ánimo de lucro) recolectan, procesan, almacenan y transmiten información en muchas formas, que incluyen los formatos electrónico, físico y las comunicaciones verbales.[22]

El valor de la información va más allá de las palabras escritas, números e imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas de información intangibles. En un mundo interconectado, la información y los procesos relacionados, los sistemas, las redes y el personal involucrado en su operación, el manejo y la protección de los activos que, como cualquier otro activo importante del negocio, son valiosos para el negocio de una organización, y en consecuencia ameritan o requieren protección contra diversos peligros. [23] [24]

Un Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas. Consta de las políticas, procedimientos, pautas y recursos y actividades asociadas, colectivamente gestionadas por una organización, en la búsqueda de la protección de sus activos de información.

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para así lograr alcanzar los objetivos de negocio.

Un sistema de gestión de seguridad de la información se basa en una identificación, evaluación, aceptación y tratamiento de riesgos, el análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para

[22] INTERNATIONAL STANDARD ISO/IEC 27000. Information security management systems — Overview and vocabulary, Third edition, 2014.
[23] INTERNATIONAL STANDARD ISO/IEC 27000. Information security management systems — Overview and vocabulary, Third edition, 2014.
[24] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información., 2009.

garantizar dicha protección, todo lo anterior contribuye a la implementación exitosa de un SGSI en una organización [25] [26]

3.2 AMENAZAS Y VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

Una amenaza tiene el potencial de causar daños a activos de información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización, algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.[27]

Una vulnerabilidad es una debilidad en cuanto a la seguridad de un activo de información o control. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla.

Fuentes de amenazas humanas: Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlar y contrarrestar sus efectos.[28]

Las fuentes de amenazas humanas abarcan actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados. Por lo anterior, es muy importante poner atención particular a las fuentes de amenazas humanas. Éstas se especifican en la Cuadro 1. Fuentes de amenazas humanas:

[25] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001. Sistemas de Gestión de la seguridad de la Información (SGSI). Requisitos, 2013.
[26] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005. Gestión del riesgo en la seguridad de la información, 2009.
[27] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005. Gestión del riesgo en la seguridad de la información, 2009.
[28] FISMA. Construcción de una Seguridad de la Información, Tecnología de sensibilización y formación. 2002.

Cuadro 1. Fuentes de amenazas humanas.

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	·Piratería ·Ingeniería social ·Intrusión, accesos forzados al sistema ·Acceso no autorizado al sistema
Criminal de la Computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	· Crimen por computador (por ejemplo, espionaje cibernético) · Acto fraudulento ·Soborno de la información ·Suplantación de identidad · Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	· Bomba/terrorismo ·Guerra* (warfare) de información ·Ataques contra el sistema (por ejemplo, negación distribuida del servicio) ·Penetración en el sistema ·Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	· Ventaja de defensa · Ventaja Política · Explotación económica · Hurto de información ·Intrusión en la privacidad personal · Ingeniería social ·Penetración en el sistema · Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)

Cuadro 1. (Continuación)

Fuente de amenaza	Motivación	Acciones amenazantes
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (por ejemplo, error en el ingreso de los datos, error de programación)	· Asalto a un empleado · Chantaje · Observar información de propietario · Abuso del computador · Soborno de información · Ingreso de datos falsos o Corruptos · Interceptación · Código malintencionado (por ejemplo, virus, bomba lógica, caballo troyano) ·Venta de información personal ·Errores (bugs) en el sistema · Sabotaje del sistema · Acceso no autorizado al sistema

Fuente: Norma técnica Colombiana NTC-ISO-IEC 27005:2009[29]

3.3 TOMA DE CONCIENCIA EN SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001:2013 en la cláusula de 7.2.2 de su anexo A, hace referencia a que todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Un programa de toma de conciencia en seguridad de la información, apunta a que las personas tomen conciencia de sus responsabilidades de seguridad de la información, y de los medios por los cuales se cumplen estas responsabilidades, este se debe alinear con las políticas y procedimientos pertinentes de seguridad de la información de la organización, teniendo en cuenta la información de la

[29] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005, 2009.

organización que se deba proteger, y los controles que se han implementado para protegerla[30].

El programa de toma de conciencia incluye varias actividades, tales como campañas, folletos y boletines de noticias. Se planifica teniendo en cuenta los roles de los empleados en la organización y en donde sea pertinente. Las actividades del programa de toma de conciencia, se planifica en el tiempo con regularidad, de manera que las actividades se repitan y abarquen a nuevos empleados y contratistas. El programa de toma de conciencia se debe actualizar regularmente, de manera que permanezca en línea con las políticas y procedimientos organizacionales, y se debería construir con base en las lecciones aprendidas de incidentes de seguridad de la información.[31]

Las campañas de sensibilización son un instrumento conformado por diversas actividades, que buscan que el usuario al interior de una organización, se encamine por las buenas prácticas en seguridad de la información, respaldando así a la organización en la responsable tarea de proteger los activos de información [32] [33]

En una campaña de sensibilización todo debe ser debidamente planificado y elaborado según sus objetivos finales, asegurando que los resultados sean los esperados por la organización, es así, que es necesario establecer indicadores que reflejen los diferentes estados de aplicabilidad de las actividades que componen la campaña.

Es importante que los empleados comprendan el objetivo de la seguridad de la información y el impacto potencial, positivo y negativo, que tiene su propio comportamiento para la organización. La toma de conciencia, la educación y la formación pueden ser parte de otras actividades de formación, por ejemplo, formación general en seguridad o en TI, o se pueden llevar a cabo en colaboración con ellas. Las actividades de toma de conciencia, educación y formación deberían

[30] MINISTERIO DE COMUNICACIONES REPÚBLICA DE COLOMBIA. Modelo de seguridad de la información para la estrategia de Gobierno en Línea, 2008. pp 7.
[31] FISMA. Construcción de una Seguridad de la Información, Tecnología de sensibilización y formación. 2002.
[32] MINISTERIO DE COMUNICACIONES REPÚBLICA DE COLOMBIA. Modelo de seguridad de la información para la estrategia de Gobierno en Línea, 2008. pp 7.
[33] SAVEDRA, O. Guía estratégica para aumentar la efectividad de las campañas de sensibilización de seguridad de la información, Revista Digital Apuntes de Investigación, Vol 3. Septiembre 2012.

ser adecuadas y pertinentes a los roles, responsabilidades y habilidades de los individuos [34]

3.4 GAMIFICACIÓN EN EL APRENDIZAJE

La utilización del juego como motivación para el aprendizaje se ha utilizado siempre en edades tempranas pero se ha estigmatizado en edades más avanzadas o incluso en la edad adulta, ya que se consideraba una pérdida de tiempo. En los últimos años se ha presentado una revalorización del juego y del aspecto lúdico ya que se ha podido constatar que su uso contribuye a desarrollar nuestra creatividad y a fijar mejor el aprendizaje debido al fuerte componente emocional. En el sitio web gamification.org se define gamificación como «El proceso de integrar los mecanismos de los juegos en entornos no lúdicos para conseguir más participación y fidelidad por parte del público, además de crear más diversión».

A simple vista podría parecer que no se trata de algo nuevo, prácticamente desde siempre, en ámbitos como la educación y el mundo de la empresa, por ejemplo, se han intentado aplicar elementos propios de los juegos para incrementar la motivación y la implicación participativa de los sujetos, para hacer la experiencia de aprendizaje o de trabajo más divertida, etc. Sin embargo, hay al menos tres factores que justifican la creciente popularización del concepto de gamificación en Internet y en el mundo académico en los últimos años.

En primer lugar, aunque los juegos siempre han formado parte de nuestra vida, tras la consolidación de la industria del videojuego (décadas de 1990 a 2000), estos han cobrado una presencia más relevante en nuestra vida cotidiana, ya no solo respecto a niños y jóvenes sino también respecto a adultos y mayores. Esto hace que la aplicación de estructuras lúdicas en cualquier contexto, más allá de los propios juegos y videojuegos, pueda ejercer, de forma más eficaz que nunca, como un puente o interfaz cultural satisfactoria y atractiva entre el individuo y el entorno en cuestión.

En segundo lugar, en los últimos años se ha expandido la gamificación a en entornos donde hasta el momento no se había dado o al menos, no se había dado de forma tan relevante y premeditada.

[34] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27002, Código de Práctica para la gestión de la seguridad de la Información, 2007.

En cuanto a la relación entre la gamificación y el diseño HCI (human-computer interaction), el auge de la Web 2.0 en los últimos años supone un ambiente muy propicio respecto a la aplicación de la perspectiva lúdica en el diseño de sitios web, para promover la implicación participativa del usuario, el incremento del tráfico, la fidelización, el desarrollo colaborativo, entre otros. En esta línea, un caso significativo sobre la aplicación de la gamificación en el (re)diseño web es el del sitio web DevHub. Se trata de un sitio web que ofrece herramientas para la construcción propia de webs y blogs a los usuarios. Según datos de los propios responsables de DevHub, hasta hace poco tiempo solo un 10 por ciento de los usuarios terminaban de completar sus sitios personales. Después de un intenso proceso de rediseño de la web a través del gamificación (basado en el libro The Art of Game Design, de J. Schell, 2008), actualmente el 80 por ciento de los usuarios termina de construir sus webs personales, de modo que la duración media de su relación con DevHub se ha prolongado exponencialmente.[35]

Por último, aunque la gamificación no sea en el fondo algo totalmente nuevo, sí lo es la base científica con la que se cuenta hoy en día para abordar su estudio y/o su implementación. En las últimas décadas, a la par del crecimiento económico y cultural del videojuego, diversos investigadores han sumado esfuerzos para empezar a construir la ciencia de las estructuras lúdicas: la Ludología, junto a la Teoría del Diseño de Juegos.[36]

De acuerdo al planteamiento anterior, se propone el uso de la gamificación como método de aprendizaje dentro de la herramienta web materia del presente trabajo de grado, teniendo en cuenta el Informe Horizon, diseñado para identificar y describir las tecnologías emergentes que puedan tener un impacto en el aprendizaje, la enseñanza y la investigación creativa en la educación superior. El Informe Horizon para el 2014 indica que en los próximos años la gamificación será una tendencia metodológica que será implementada en el entorno académico.

3.5 CARACTERÍSTICAS FUNDAMENTALES DE LA GAMIFICACIÓN

El elemento esencial de la gamificación es la combinación entre un entorno con reglas muy claramente definidas y una experiencia del usuario con amplia libertad

[35] ZICHERIMANN, Gabe. Gamification by Design: Implementing Fame Mechanics ub web and mobile apps. Sebastopol: O'Reilly, 2011, p. 15
[36] ZICHERIMANN, Gabe. Gamification by Design: Implementing Fame Mechanics ub web and mobile apps. Sebastopol: O'Reilly, 2011, p. 16

de interacción dentro de esas reglas. Un segundo elemento esencial del juego es la cualidad participativa de la experiencia del usuario.

Por otro lado, la interactividad lúdica se caracteriza también por la posibilidad de volver atrás y explorar caminos alternativos o, al menos, intentar mejorar la destreza ante un determinado reto del juego. Si bien la actividad repetitiva en la vida cotidiana suele experimentarse de forma negativa, en los juegos y los videojuegos la repetición va siempre asociada al aprendizaje, una visibilidad clara de la evolución de nuestro rendimiento (sistemas de puntuación, rankings, etc.) e incluso, en muchos casos, el descubrimiento de nuevos caminos posibles.

Un cuarto rasgo fundamental del juego es el hecho de que este proporciona al jugador una experiencia metafórica de descubrimiento y adaptación a un mundo desconocido. En este sentido, desde el análisis psicológico del juego, se destaca que una de las cualidades esenciales del juego es el hecho de que, para tener éxito, el jugador necesita integrarse como individuo en una estructura ajena.

Finalmente, en la gamificación se identifican principalmente las siguientes dinámicas de juego[37]:

- Recompensa: La recompensa es un incentivo para la realización de una tarea, el jugador se sentirá más atraído hacia el juego.

- Estatus: Ser miembro de una comunidad y posicionarse en esta motiva a seguir jugando.

- Reconocimiento: Una persona se distingue entre las demás, por ejemplo, por jugar con una buena estrategia. Las personas se sienten comprometidas con actividades que les proporcionan reconocimiento.

- Expresión y autoexpresión: El jugador quiere expresar su identidad, su autonomía, su personalidad y su originalidad ante los demás jugadores.

- Competición: La competición es la práctica de un juego que tiene como resultado una clasificación de los participantes. La comparación con los demás es una fuente de motivación para muchos jugadores.

[37] ROMERO, Hairol y ROJAS, Elvin. La Gaminificación como participante del B-Learning: Su percepción en la Universidad Nacional, sede Regional Brunca, Costa Rica. 2013

- Juego cooperativo: Dos o más jugadores no compiten; se esfuerzan por conseguir un mismo objetivo, un mismo fin.

- Altruismo: Las personas se esmeran en ayudar a otras o apoyar causas solidarias sin esperar una recompensa a cambio.[38]

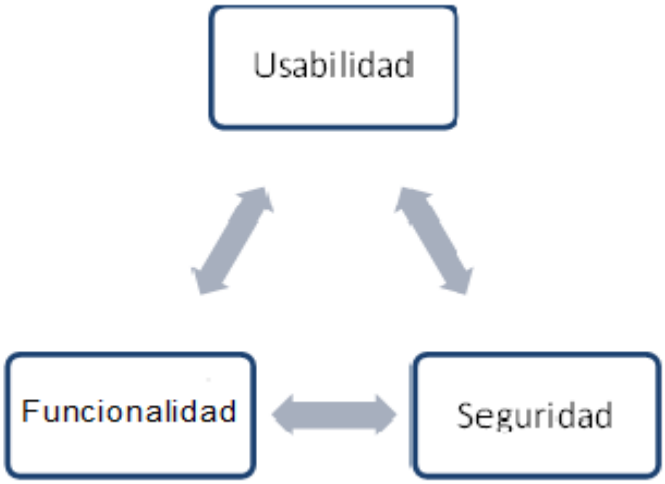
[38] ROMERO, Hairol y ROJAS, Elvin. La Gaminificación como participante del B-Learning: Su percepción en la Universidad Nacional, sede Regional Brunca, Costa Rica. 2013

4. DISEÑO DE LA HERRAMIENTA

Como parte del diseño de la herramienta web, que tiene como objetivo lograr una sensibilización eficaz de las personas respecto a temas relacionados con seguridad de la información, ciberseguridad y un Sistema de Gestión de Seguridad de la Información (SGSI), es necesario evaluar las herramientas y lenguajes de programación de los cuales se dispone para la construcción de la aplicación web.

De acuerdo a las directrices sugeridas por el EC-Council para evaluación y creación de aplicaciones se busca que la aplicación tenga una armonía entre usabilidad, funcionalidad y seguridad, tal como se muestra en la figura 2. Directrices para la evaluación y creación de aplicaciones.

Figura 2. Directrices para la evaluación y creación de aplicaciones.



Fuente: Elaboración propia.

Estás características están definidas por:

- Usabilidad: Que la aplicación tenga una interfaz agradable, sea fácil de usar y sea intuitiva para el usuario final. Para esto la aplicación presenta una interfaz agradable y con configuraciones de estilo grafico personalizable, logrando así

cambiar logos, fondos, colores, fuentes entre otras y además usando secuencias predecibles sobre los diferentes pasos a seguir en la aplicación.

- Funcionalidad: Que la aplicación cumpla con su objetivo, que sea rápida y eficaz. En este caso la aplicación busca brindar conocimientos de seguridad de la información de una manera amigable, social y competitiva.

- Seguridad: Que la información que se almacena y procesa en la aplicación tenga niveles óptimos en cuanto a su integridad, disponibilidad y confidencialidad, así como también que se respete la privacidad del usuario. Para esto se implementa manejo de sesiones, contraseñas, validación de correos.

El desarrollo de aplicaciones web en la actualidad se realiza utilizando frameworks de desarrollo, que son herramientas diseñadas para apoyar la construcción de software, básicamente son un conjunto de librerías y scripts que se encargan de realizar tareas comunes a la mayoría de aplicaciones web, como son manejo de sesión de usuarios, acceso a bases de datos y plantillas, por mencionar algunas. Además de facilitar la reutilización de código, estos frameworks alivian el exceso de carga de desarrollo y al ahorrar una cantidad significativa de tiempo permiten que el equipo de trabajo se pueda enfocar en las partes de la aplicación que son únicas a sus objetivos.

Teniendo en cuenta lo anterior, se realizó un proceso de comparación de diferentes frameworks de desarrollo web. Con el fin de escoger un framework que se ajuste a las necesidades específicas del proyecto, se realizó una exploración de las distintas opciones que podrían servir para el proceso de implementación.

Los factores de comparación que se tienen en cuenta para determinar la mejor opción son los siguientes:

- Licencia: La licencia puede ser libre, privativa o abierta. Según el caso se podría requerir de un pago por el uso de la herramienta. Adicionalmente la licencia influye en términos de soporte de la herramienta.

- Última Versión Estable: Es un buen indicador de la actualidad de la herramienta, se buscan herramientas con versiones estables recientes que indiquen que son producto de un trabajo activo.

- Sistema Operativo: Es importante saber qué sistema operativo requiere la herramienta, pues esto también podría implicar un costo de licenciamiento o actualización de equipos de desarrollo o despliegue de la herramienta al momento de ser implementada y publicada.

- Lenguaje: Este es uno de los parámetros más importantes de la comparación, ya que el lenguaje en el que está escrita la herramienta será el mismo en el que se deba escribir el desarrollo, al menos en su mayor parte. Esto quiere decir que al escoger una herramienta software de un lenguaje específico inmediatamente estamos recibiendo las ventajas o desventajas que pueda tener este lenguaje.

- Arquitectura: La arquitectura del software es la organización fundamental del sistema que incluye a sus componentes, sus relaciones entre ellos así como el ambiente y los principios que dictan su diseño y evolución <IEEE 1471-2000 - Booch, Kruchten, Reitman, Bittner, and Shaw> La arquitectura que se utilice para el desarrollo de la aplicación tiene una importancia primordial ya que influye directamente en características fundamentales como escalabilidad, mantenimiento, modularidad y complejidad.

- Soporte Para Bases De Datos: La persistencia de los datos utilizados por la aplicación, es una de estas tareas comunes que pueden significar una gran carga de desarrollo, es por esto que es importante que el framework escogido cuente con un soporte confiable para diferentes bases de datos y facilite su interacción desde la lógica de la aplicación.

- Documentación: Tener una buena cantidad de documentación disponible para una herramienta es un factor que permite darle un mejor uso y facilitar el aprendizaje de la misma. Es importante que la herramienta escogida cuente con una documentación accesible y de calidad.

- Librerías: La librerías son porciones de código que se encargan de realizar tareas específicas y que pueden ser utilizadas por otras piezas de software. Un framework de desarrollo que cuente con una gran variedad de librerías permitirá realizar más tareas de forma automática sin necesidad de volverlas a escribir.

4.1 FRAMEWORKS DE DESARROLLO

A continuación se muestra una comparativa que relaciona los diferentes frameworks estudiados teniendo en cuenta los factores anteriormente descritos:

4.1.1 Jboss

- Licencia: LGPL, licencia libre que además brinda la libertad de compartir y modificar el software cubierto por ella.

- Última Versión Estable: 7.1.1 de marzo de 2012

- Sistema Operativo: Multiplataforma

- Lenguaje: JAVA

- Arquitectura: Orientada a Servicios (SOA)

- Soporte Para Bases De Datos: Se configura por medio de archivos .xml y se deben instalar manualmente drivers .jar. Es necesario establecer las conexiones a bases de datos desde el código de la aplicación. Soporta bases de datos IBM, Oracle, MySQL, Microsoft SQL y PostgreSQL.

- Documentación: La documentación encontrada está en su mayoría en inglés y tiene dos o más años de antigüedad, lo cual tiene directa relación con la fecha de la última versión estable.

- Librerías: Cuenta con una buena cantidad de librerías escritas en JAVA, pero muchas de ellas están desactualizadas y pueden presentar problemas de incompatibilidad.

4.1.2 Django

- Licencia: 3-clause BSD, está licencia es libre y además permite el uso del código fuente en software no libre.

- Última Versión Estable: 1.7.1 de octubre 22 de 2014

- Sistema Operativo: Multiplataforma

- Lenguaje: Python

- Arquitectura: Modelo Vista Controlador (MVC)

- Soporte Para Bases De Datos: Se deben instalar drivers y configurar parámetros de configuración en un archivo python. Permite manejar la información de la base de datos como si fueran objetos. Soporta bases de datos PostgreSQL, MySQL y SQLite.

- Documentación: En Internet está disponible una gran cantidad de información actualizada y de calidad generada por usuarios alrededor del mundo mediante foros, listas de correo, documentación oficial y traducciones.

- Librerías: Tiene a su disposición todas las librerías de Python, uno de los lenguajes más populares y más utilizados de la actualidad.

4.1.3 Drupal

- Licencia: GPLv2/GPLv3, licencias ampliamente usadas y ampliamente difundidas, estás licencias garantizan la libertad de usar, estudiar, compartir (copiar) y modificar el software.

- Última versión estable: 7.34 de 19 de noviembre de 2014

- Sistema operativo: Multiplataforma

- Lenguaje: PHP

- Arquitectura: Sistema de Gestión de Contenidos (CMS)

- Soporte para bases de datos: Toda la información de Drupal está guardada en una base de datos que se accede por medio de una interfaz gráfica o comandos SQL. Soporta bases de datos MySQL, PostgreSQL, SQLite, Microsoft SQL Server, Oracle y MongoDB.

- Documentación: Buena cantidad de información generada por una gran comunidad de habla hispana activa en foros, cuentas de correo y documentos oficiales.

- Librerías: La funcionalidad de Drupal se puede extender por medio de módulos programados por su comunidad de usuarios. En agosta de 2012 en la página oficial de Drupal se listan 17.644 módulos libres.

4.1.4 Symfony

- Licencia: Licencia MIT, Licencia de “Massachusetts Institute of Technology”, esta licencia permite reutilizar el software con licencia MIT tanto para construir software libre como para ser software no libre.

- Última versión estable: 2.6.3 de 7 de enero de 2015

- Sistema operativo: Multiplataforma

- Lenguaje: PHP

- Arquitectura: Modelo Vista Controlador (MVC), arquitectura que separa la interfaz gráfica del usuario, la lógica del sistema y los datos.

- Soporte para bases de datos: Se utiliza una librería llamada Doctrine para el acceso y manejo de la información de la base de datos. Permite manejar la información de la base de datos como si fueran objetos. Soporta bases de datos MySQL, PostgreSQL, Oracle y Microsoft SQL Server.

- Documentación: Está publicado un Libro oficial y existen grupos activos en internet que mantienen una documentación oficial actualizada en español.

- Librerías: La funcionalidad de Symfony se puede extender fácilmente con código propio, o con funciones de otros frameworks y librerías escritas en php.

4.1.5 Ruby on rails

- Licencia: Licencia MIT
- Última versión estable: 4.1.6 de 12 de septiembre de 2014
- Sistema operativo: Multiplataforma
- Lenguaje: Ruby
- Arquitectura: Modelo Vista Controlador (MVC)
- Soporte para bases de datos: El acceso a base de datos es totalmente abstracto desde el punto de vista del programador, Rails gestiona los accesos a la base de datos automáticamente y permite manejar la información de la base de datos como si fueran objetos. Soporta bases de datos MySQL, PostgreSQL, SQLite, IBM, DB2 y Oracle.
- Documentación: Existe una buena documentación en español, manuales, libros virtuales y cursos online.
- Librerías: La funcionalidad de Rails se puede extender utilizando piezas de software escritas en Ruby llamadas Gemas.

4.2 COMPARACIÓN ENTRE FRAMEWORK

- Licencia: Al realizar la exploración de las diferentes opciones según los parámetros establecidos se encontró que todas las licencias utilizadas son licencias de código abierto o libre que permiten su uso sin incurrir en costos económicos, razón por la cual la licencia no se toma como un factor decisivo de importancia.
- Sistema operativo: Igualmente sucede con el sistema operativo, ya que todas las herramientas son multiplataforma, es decir, su uso no está restringido a un sistema operativo específico.
- Última versión estable: En cuanto a las últimas versiones estables se tiene que todas las herramientas, excepto Jboss se encuentran actualizadas en fechas recientes.

- Soporte para bases de datos: En general todas las opciones soportan diversos motores de bases de datos, por lo que la característica más importante de este factor es la capacidad de manejar la información de la base de datos como si fueran objetos, ofrecida por Rails, Symfony y Django. Esto permite una interacción más transparente con los datos durante el desarrollo de la aplicación.

- Documentación: Todas las opciones estudiadas cuentan con una buena documentación, excepto JBoss. Se destaca Django por la calidad de la documentación oficial y la actividad de los diferentes grupos de usuarios en Internet.

- Librerías: Los frameworks con una mejor oferta de librerías son Django y Rails. Esto garantiza una amplia gama de funcionalidades que se pueden utilizar de forma automática durante el desarrollo.

- Arquitectura: Los frameworks analizados implementan tres tipos de arquitecturas: Orientada a Servicios (SOA), Modelo Vista Controlador (MVC) y Sistema de Gestión de Contenidos (CMS).

SOA es un estilo de Arquitectura de Software basado en la definición de servicios reutilizables, con interfaces públicas bien definidas, donde los proveedores y consumidores de servicios interactúan en forma desacoplada para realizar los procesos de negocio. Se basa en cuatro abstracciones básicas: servicios, application frontend, repositorio de servicios y bus de servicios. Un servicio consiste en una implementación que provee lógica de negocio y datos, un contrato de servicio, las restricciones para el consumidor, y una interfaz que expone físicamente la funcionalidad. Las application frontend consumen los servicios formando procesos de negocios. Un repositorio de servicios almacena los contratos de servicios y el bus de servicios interconecta las application frontend y los servicios.[39]

Los servicios representan grupos lógicos de operaciones relacionadas con algún concepto del negocio. Por su parte, los procesos del negocio se realizan en servicios orientados a procesos que se componen de secuencias definidas de invocaciones

[39] DELGADO, Andrea, GONZÁLEZ, Laura yPIEDRABUENA, Federico. Desarrollo de aplicaciones con enfoque SOA (Service Oriented Architecture) Instituto de Computación – Facultad de Ingeniería Universidad de la República Montevideo, Uruguay, 2006.

a servicios, mediante una orquestación de los mismos en lo que se conoce como coreografías de servicios.[40]

La arquitectura Modelo Vista Controlador es un tipo de arquitectura software que divide la aplicación en tres partes interconectadas con el fin de separar los datos y la lógica de negocio de una aplicación de la interfaz de usuario y el módulo encargado de gestionar los eventos y las comunicaciones. La primera de estas tres partes es el Modelo, que captura el estado de la aplicación, maneja su lógica y reglas y es independiente de la interfaz de usuario; el segunda son las vistas, las cuales son la representación de cualquier información de la aplicación que se muestra al usuario, y finalmente los controladores son los elementos encargados de recibir las entradas y convertirlas en comandos para el modelo o la vista.

Un Sistema de Gestión de Contenidos consiste en una estructura que permite controlar una base de datos en la que se aloja el contenido de un sitio web. Sobre este contenido web se pueden realizar diferentes tareas de mantenimiento teniendo en cuenta diferentes niveles de autenticación de usuario y permisos.

Luego de hacer un estudio sobre las diferentes arquitecturas ofrecidas, se determinó que el Sistema de Gestión de Contenidos no es una buena opción debido a lo limitado de sus capacidades, la arquitectura Basada en Servicios presenta una complejidad adicional en su diseño, lo que aumentaría la carga del proceso de desarrollo en lugar de facilitar el proceso. Es por esto que se elige trabajar con la arquitectura Modelo Vista Controlador, ofrecida por los frameworks Symfony, Rails y Django.

- Lenguaje: El principal factor determinante a la hora de decidir qué framework utilizar fue el lenguaje de programación utilizado. Las tres opciones disponibles: Python, PHP y Ruby son los lenguajes de programación más utilizados en la actualidad, sin embargo, cada uno presenta diferentes ventajas y desventajas.

PHP es un lenguaje de programación fácil de aprender, con una gran comunidad de usuarios y puede ser utilizado en una gran cantidad de servidores web, sus desventajas principales son: manejo de errores poco eficiente, complejidad en la puesta en producción y poca portabilidad.

[40] DELGADO, Andrea, GONZÁLEZ, Laura yPIEDRABUENA, Federico. Desarrollo de aplicaciones con enfoque SOA (Service Oriented Architecture) Instituto de Computación – Facultad de Ingeniería Universidad de la República Montevideo, Uruguay, 2006.

Python es un lenguaje de alto nivel multipropósito ampliamente utilizado. Se destaca por su facilidad de lectura y similitud con el pseudo-código. Es fácil de aprender y presenta una sintaxis organizada que permite un rápido despliegue de prototipos, poniendo en práctica una efectiva reutilización de código por medio de módulos y paquetes. Python presenta desventajas en cuanto a su rapidez, pues no soporta tareas con múltiples procesadores de manera óptima.

Ruby es también un lenguaje de alto nivel, multipropósito, totalmente orientado a objetos con técnicas de manipulación de cadenas de texto avanzadas y una sintaxis flexible. La principal desventaja de Ruby tiene que ver con la dificultad que implica su aprendizaje, soporte y documentación.

4.3 ELECCIÓN DEL FRAMEWORK.

Teniendo en cuenta las diferentes comparaciones realizadas anteriormente y las características que cada framework representa, se escoge como herramienta de desarrollo el framework Django escrito en Python porque presenta una arquitectura adecuada a las necesidades del proyecto (Modelo Vista Controlador), ofrece una gran cantidad de funcionalidades y librerías, es de fácil aprendizaje y además cuenta con buenas fuentes de documentación actualizada.

4.4 ANÁLISIS DE REQUERIMIENTOS

Con el fin de establecer una base de información a partir de la cual se realice el diseño, implementación y prueba de la aplicación se definen los requerimientos no funcionales y los requerimientos funcionales que debe cumplir el software.

4.4.1 Requerimientos no funcionales. A continuación se listan los requerimientos no funcionales que expresan las propiedades o cualidades que debe tener la aplicación:

- El contenido de la aplicación debe estar basado en estándares internacionales, recomendaciones, buenas prácticas y casos reales o noticias que estén orientadas a generar impacto en el usuario, para adquirir compromiso, conciencia y cultura con la seguridad de la información.

- La aplicación debe brindar un mecanismo donde el usuario pueda evaluar sus conocimientos en seguridad de la información y al mismo tiempo aprender más sobre este tema, de tal forma que se convierta en una herramienta útil en campañas

de sensibilización para generar conciencia y cultura sobre seguridad de la información.

- La aplicación debe incorporar mecánicas de juego (gamificación) para mejorar y facilitar el aprendizaje de conceptos, situaciones, buenas prácticas y en general preguntas relacionadas con la seguridad de la información, mediante un sistema de puntuaciones, rankings y barras de progreso que consiguen que el aprendizaje sea más ameno, divertido y entretenido, la aplicación debe usar técnicas de motivación basadas en redes sociales centrado en aprender – fallando.

- La interfaz de usuario debe ser simple e intuitiva para que sea fácil de manejar y amigable para el usuario final.

- La interfaz de la aplicación debe permitir ubicar un logo de organización en un lugar visible.

- La velocidad de respuesta de la aplicación debe ser tal que permita a varios usuarios utilizarla de forma simultánea sin que se genere una mala experiencia.

- La aplicación debe tener un módulo de administración para la información con que se alimenta la aplicación se pueda gestionar de manera adecuada, rápida y sencilla.

4.4.2 Requerimientos funcionales. Los requerimientos funcionales son las acciones que debe ser capaz de realizar el sistema y especifican las transformaciones que el sistema realiza sobre las entradas para producir las salidas.

Funciones del Sistema:

- El sistema debe permitir crear, editar y eliminar perfiles de usuarios.

- El correo electrónico debe ser único para cada usuario.

- El sistema debe enviar un mensaje de error, cuando se intente sobrepasar el número máximo de usuarios permitidos.

- El sistema debe permitir la creación de organizaciones con un número máximo de usuarios asignado.

- El sistema debe permitir crear, editar y eliminar categorías de preguntas.

- El sistema debe permitir crear, editar y eliminar preguntas de diferentes tipos (selección múltiple, falso o verdadero, completar) y asociarlas a categorías existentes.

- El sistema debe permitir asignar categorías de preguntas a los usuarios por medio de las organizaciones a las que pertenecen.

- El sistema debe permitirles a los usuarios responder las preguntas de las categorías que le hayan sido asociadas.

- El sistema debe asignar a cada usuario una puntuación que depende de su desempeño al responder las preguntas. Cada pregunta correcta asigna 10 puntos, cada respuesta equivocada resta 5 puntos, si el usuario no tiene puntos no se restan, es decir, el mínimo número de puntos es 0.

- El sistema debe llevar un registro de las preguntas contestadas por el usuario.

- El sistema debe asignar a cada usuario una medalla por cada categoría de preguntas completada.

- El sistema debe medir el desempeño de los usuarios al responder las preguntas y permitir que se identifique a un usuario como el mejor y mostrarlo en un ranking de usuarios por organización

- El sistema debe permitir una visualización de prueba de 3 preguntas (trial)

- El sistema no debe permitir visualizar a los usuarios, preguntas de categorías que no estén autorizadas por el administrador.

- El sistema no debe permitir la modificación de la puntuación de los usuarios para así evitar fraudes.

- El sistema debe explicar las respuesta a cada pregunta realizada a al usuario.

- El sistema no debe permitir que cuentas de usuarios de organizaciones accedan al módulo administración, por lo cual el sistema debe contar con módulos de acceso independientes para estos dos actores.

4.5 REQUERIMIENTOS DE SISTEMA

Para que el sistema pueda realizar las tareas especificadas en los puntos anteriores, se requieren los siguientes componentes:

- Navegador web por medio del cual el usuario hace uso de la aplicación.

- Servidor web configurado para soportar aplicaciones Django, donde se almacena el código de la aplicación.

- Base de datos que permita almacenar de forma persistente la información de la aplicación.

4.6 CASOS DE USO

A continuación se enumeran los casos de uso basados en los actores, es decir, agentes externos que interactúan con el sistema. Cada caso de uso representa la forma en que uno o varios actores usan el sistema para lograr un objetivo.

Para definir la interacción con la aplicación se definieron tres tipos de actores de acuerdo a las actividades que realizan, los actores definidos son: usuario, administrador y usuario tester. Su interacción con la aplicación es la siguiente:

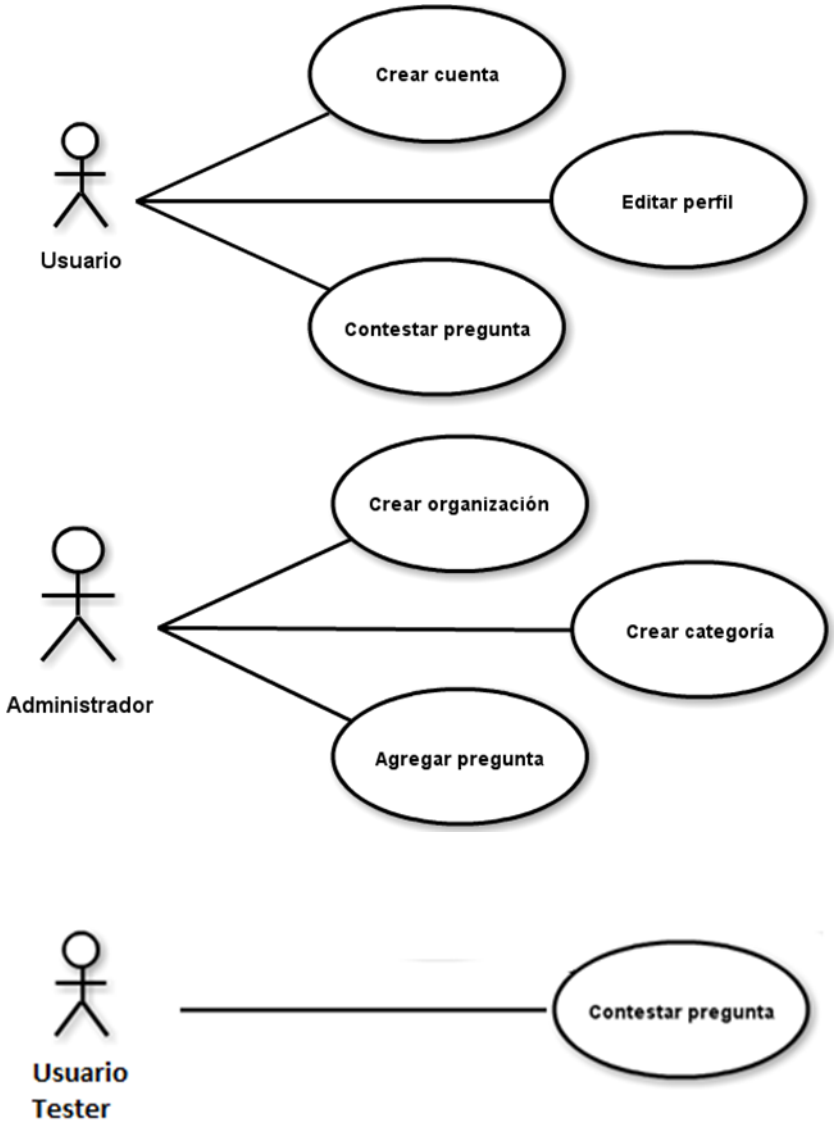
- Usuario: Es la persona perteneciente a una organización quien será el público objetivo de la aplicación.

- Administrador: Es la persona quién se encargará del alistamiento, parametrización y configuración de la aplicación.

- Usuario tester: Persona interesada en conocer la funcionalidad de la aplicación.

Los actores del sistema y sus casos de usos se representan en la Figura 3.Casos de uso del sistema.

Figura 3. Casos de uso del sistema.



Fuente: Elaboración propia.

4.6.1 Caso de uso: crear cuenta de usuario.

- Actor: Usuario.

- Sinopsis: El usuario ingresa por primera vez a la aplicación y crea una cuenta de usuario con un perfil asociado.

- Curso típico de eventos:

1. El usuario accede a la aplicación y da clic en opción “Log In” de la barra superior.
2. El usuario escoge la opción “Registrarse”.
3. El usuario ingresa su nombre de usuario, correo electrónico, contraseña con confirmación y da clic en el botón “Registrarse”. Por medio del correo electrónico se determina la organización a la que pertenece el usuario.
4. El usuario elige completar perfil e ingresa su información personal adicional (nombre y un mensaje personal) junto con una imagen de perfil opcional.
5. El usuario es dirigido a su página de perfil donde encontrará un panel con su imagen de perfil, información de usuario y puntaje, un ranking de los mejores usuarios de la organización, y una serie de categorías de preguntas que debe responder en las cuales debe lograr conocer las categorías terminadas (medallas obtenidas) o el progreso en cada una de ellas.

- Curso Alternativo de Eventos:

1. En el punto 3 puede ocurrir que la organización haya completado el número máximo de usuarios asignados, en caso tal el usuario es notificado con un mensaje que le informa la situación y no se puede continuar el proceso de registro.
2. El en punto 3 puede ocurrir que el correo del usuario no corresponda a ninguna organización existente en el sistema, en caso tal el usuario es notificado con un mensaje que le informa la situación y no se puede continuar el proceso de registro.

4.6.2 Caso de uso: editar perfil

- Actor: Usuario.

- Sinopsis: El usuario modifica su información personal.

- Curso Típico de Eventos:

1. El usuario inicia sesión y es dirigido a su página de perfil
2. El usuario elige la opción “editar perfil”
3. El usuario modifica su imagen de perfil o su mensaje personal
4. El usuario elige la opción “Actualizar perfil”, se guardan los cambios y es redirigido a su página de perfil.

- Curso Alternativo de Eventos:

1. En el punto 3 el usuario puede elegir la opción “cambiar contraseña”, en tal caso se le presenta un formulario para que ingrese su contraseña antigua y una nueva contraseña con confirmación.
2. En el punto 4 el usuario puede elegir la opción “volver”, en tal caso se redirige a la página de perfil sin alterar su información.

4.6.3 Caso de uso: contestar pregunta

- Actor: Usuario.

- Sinopsis: El usuario ingresa a una categoría y responde una pregunta.

- Curso Típico de Eventos:

1. Si el usuario tester es quien inicia el caso de uso, pasa al paso 5.
2. El usuario inicia sesión y es dirigido a su página de perfil.
3. El usuario elige una categoría haciendo clic en el nombre de la categoría ubicado sobre la barra de progreso de la misma.
4. El usuario es dirigido a una página donde se le muestra una pregunta de la categoría escogida que aún no ha respondido de forma correcta, teniendo en cuenta el progreso que llevaba la última vez que respondió preguntas de esta categoría.
5. El usuario elige la respuesta según el tipo de pregunta (selección múltiple, completar, falso o verdadero) y la envía dando clic en el botón “siguiente/responder”.
6. El usuario recibe la calificación de su pregunta y un texto explicativo de la calificación, si esta es correcta su puntaje aumenta en 10 puntos, si su es incorrecta, disminuye en 5 puntos.
7. El usuario da clic en el botón “siguiente/responder” para continuar y se redirige a una página donde se muestra otra pregunta de la categoría que aún no ha contestado correctamente, elegida de forma aleatoria.

8. Se repiten los puntos 4 – 6 hasta que el usuario responda todas las preguntas pendientes de la categoría o de clic en el botón “volver” para volver a la página de perfil.

- Curso Alternativo de Eventos:

1. En el punto 4 el usuario puede olvidar ingresar una respuesta antes de dar clic al botón, en tal caso se le muestra una notificación que le solicita escoger una respuesta.
2. En el punto 4 el usuario puede elegir dar clic en el botón “volver” para regresar, en tal caso se regresa a la página de perfil sin modificar su progreso en la categoría.
3. En el punto 6 se puede dar que la pregunta que se acaba de responder de forma correcta era la última pregunta pendiente de la categoría, en este caso al usuario se le notifica que ha terminado una categoría y por lo tango ganado la medalla correspondiente y se redirige a la página de perfil.

4.6.4 Caso de uso: crear organización

- Actor: Administrador.

- Sinopsis: El administrador crea una nueva organización con un número máximo de usuarios asignados.

- Curso Típico de Eventos:

1. El administrador inicia sesión con sus credenciales en el panel de administración
2. El administrador va a la sección organizaciones y elige la opción “Añadir organización”
3. El administrador ingresa el nombre de la nueva organización y si lo desea también agrega una imagen y una descripción
4. El administrador establece el máximo número de usuarios que tendrá la organización
5. El administrador guarda la información de la nueva organización

4.6.5 Caso de uso: crear categoría

- Actor: Administrador.

- Sinopsis: El administrador crea una nueva categoría de preguntas y la asigna a una o más organizaciones.

- Curso Típico de Eventos:

1. El administrador inicia sesión con sus credenciales en el panel de administración.
2. El administrador va a la sección categorías y elige la opción “Añadir categoría”.
3. El administrador ingresa el nombre, una imagen y descripción opcionales de la categoría.
4. El administrador elige las organizaciones a las cuales asigna esta categoría de una lista de las organizaciones existentes en el sistema.
5. El administrador guarda la nueva categoría.

4.6.6 Caso de uso: agregar pregunta

- Actor: Administrador.

- Sinopsis: El administrador elige una categoría existente y agrega una pregunta que puede ser de selección múltiple, falso o verdadero o de completar.

- Curso Típico de Eventos:

1. El administrador inicia sesión con sus credenciales en el panel de administración.
2. El administrador va a la sección categorías y escoge una de las categorías existentes.
3. El administrador selecciona el tipo de pregunta que desea agregar.
4. El administrador ingresa la información necesaria según el tipo de pregunta.
5. El administrador guarda los datos de la nueva pregunta.

4.7 CASOS DE ABUSO

Los casos de abuso describen el comportamiento del sistema bajo posibles patrones de ataque a los que puede estar expuesta la aplicación en un ambiente de producción. Esto permite determinar si el diseño propuesto mitiga los riesgos identificados.

Los casos de abuso identificados se presentan en el Cuadro 2. Casos de abuso del sistema.

Cuadro 2. Casos de abuso del sistema.

Caso de Abuso	Control	Mitigación de la amenaza
Creación de cuentas de correo falsas	El sistema realiza una validación del dominio al que pertenece la cuenta de correo, si el dominio no está autorizado no se permite la creación de la cuenta	Amenaza mitigada por medio del diseño de la aplicación
Ingreso a cuentas de otros usuarios	El sistema protege el acceso de usuarios por medio de validación de contraseñas seguras y uso de SSL en producción	Amenaza mitigada por medio del diseño de la aplicación
Inyección de código malicioso	El sistema cuenta con procesos de validación de formularios que previenen ataques CSRF o XSS	Amenaza mitigada por medio del diseño de la aplicación
Acceso no autorizado a bases de datos	En el sistema el único usuario que puede acceder directamente a la base de datos es el administrador, perfil protegido con una contraseña segura y con ruta de acceso privada	Amenaza mitigada por medio del diseño de la aplicación
Manipulación de información de otros usuarios	La aplicación cuenta con un sistema de manejo de sesiones robusto que utiliza cifrado para prevenir ataques de session hijacking	Amenaza mitigada por medio del diseño de la aplicación

Cuadro 2. (Continuación)

Caso de Abuso	Control	Mitigación de la amenaza
Alteración de integridad de los datos	El sistema cuenta con un esquema de bases de datos robusto que protege su integridad por medio de validaciones como tipos de datos específicos, campos requeridos y valores por defecto	Amenaza mitigada por medio del diseño de la aplicación
Denegación de servicios	Aunque la aplicación está diseñada para soportar un nivel de tráfico mayor al esperado, los controles que establece para este caso no pueden mitigar este riesgo	El sistema debe apoyarse en infraestructura de red como firewalls para mitigar el riesgo de denegación de servicios

Fuente: Elaboración propia.

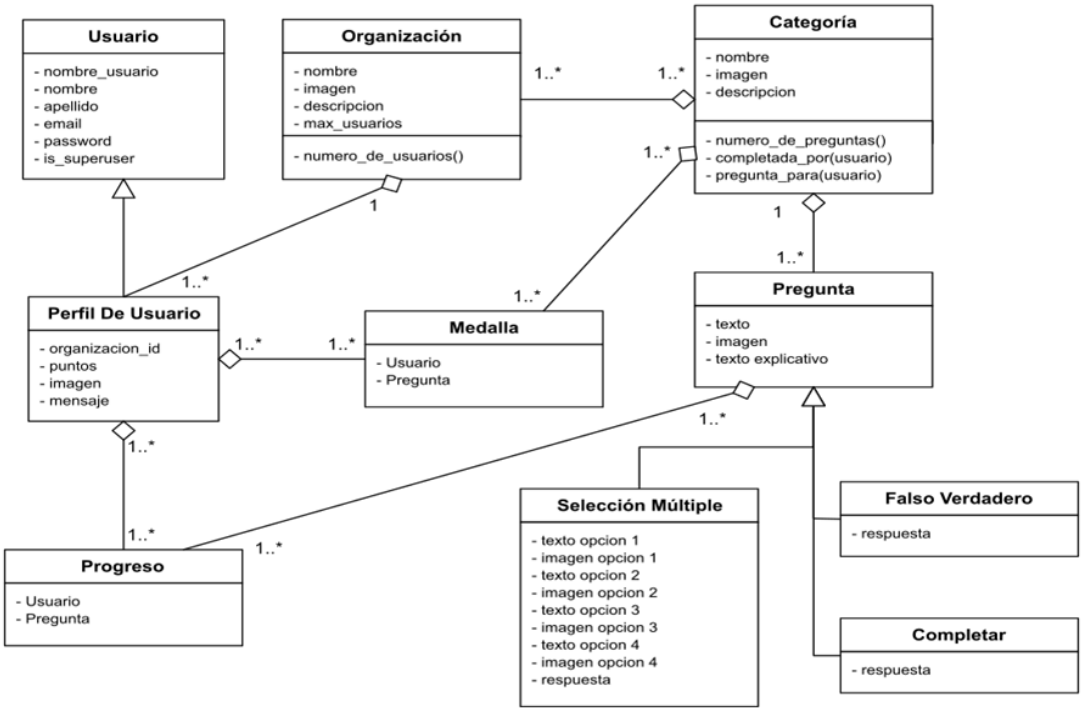
4.8 DIAGRAMA DE CLASES

En la Figura 4. Diagrama de clases del sistema, se muestra el diagrama de clases de la aplicación, en él se pueden apreciar las diferentes relaciones entre las clases de objetos, sus atributos y métodos, que representan la estructura del sistema.

Las clases que conforman el sistema son:

- Usuario
- Perfil de Usuario
- Organización
- Categoría
- Pregunta
- Pregunta Falso o Verdadero
- Pregunta Selección Múltiple
- Pregunta Completar
- Progreso
- Medalla

Figura 4. Diagrama de clases del sistema.

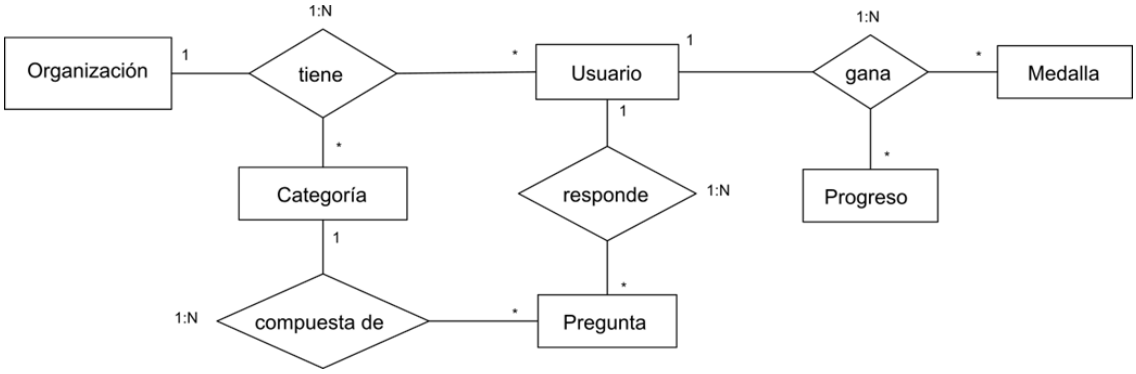


Fuente: Elaboración propia.

4.9 DIAGRAMA DE BASE DE DATOS

En la Figura 5. Diagrama de Base de datos, se presenta el diagrama de las entidades más relevantes del sistema, sus relaciones y propiedades. Como entidades relevantes del sistema se consideran Organización, Categoría, Usuario, Pregunta, Medalla y Progreso.

Figura 5. Diagrama de Base de datos.

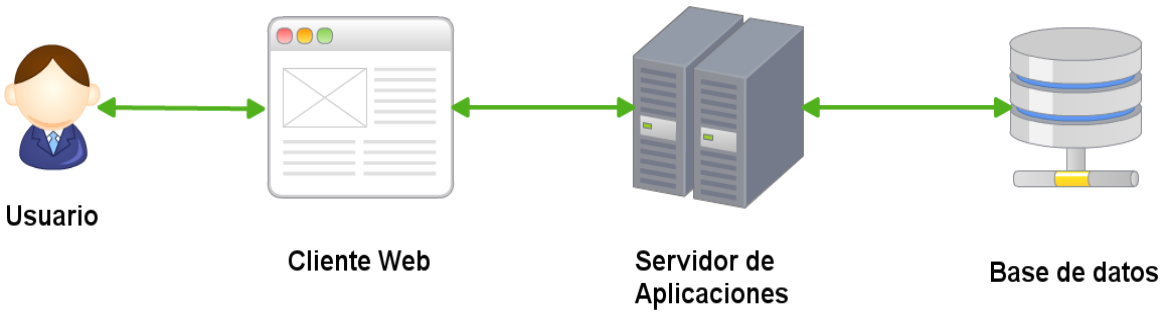


Fuente: Elaboración propia.

4.10 ESTRUCTURA DE LA APLICACIÓN

La estructura de la aplicación se puede dividir en tres niveles como los que se muestran en la Figura 6. Estructura de la aplicación.

Figura 6. Estructura de la aplicación.



Fuente: Elaboración propia.

- Cliente web: Al ser esta una aplicación web, la interacción del usuario con el sistema se realiza por medio de un cliente web, que puede ser cualquier navegador web a través del cual el usuario podrá ver la información entregada por la aplicación y a su vez ingresar la información necesaria para darle uso.

- Servidor de aplicaciones: El cliente web se encarga de transmitir y dar formato a la información haciendo de intermediario entre el usuario y el servidor de aplicaciones. Es en este servidor de aplicaciones donde está instalada la aplicación Django y es quien se encarga de la lógica del sistema y de interactuar con la base de datos.

- Base de datos: La base de datos es la parte del sistema que permite darle persistencia a la información y mantener de forma íntegra el estado de la misma. En el ambiente de desarrollo para la base de datos se utiliza un motor Sqlite3 de fácil configuración, pero en producción es necesario un motor de mejor desempeño como MySQL.

5. MÓDULOS DESARROLLADOS

Como resultado del diseño se desarrolla la herramienta Web orientada a generar conciencia y cultura sobre la seguridad de la información. La aplicación está diseñada para prestar un servicio, de tal forma que pueda soportar a varias organizaciones, por lo cual se discriminan los módulos de administración y usuario.

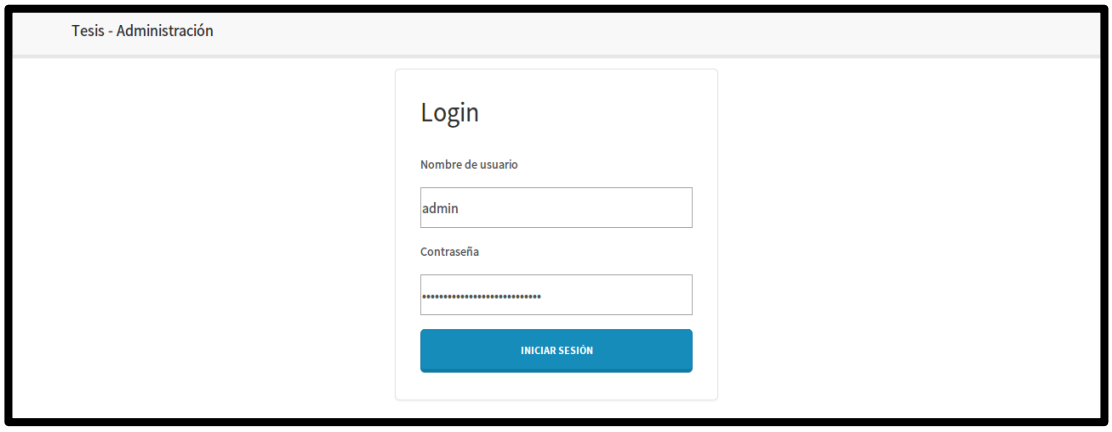
5.1 MÓDULO ADMINISTRADOR

El administrador es quien ingresa la información básica necesaria para que el sistema funcione, se encarga de crear las diferentes organizaciones, categorías y preguntas, así como de asignar las diferentes categorías a las organizaciones. También puede ver y editar la información almacenada en la base de datos.

El módulo de administración no pertenecerá a una organización en particular, dado que la herramienta está pensada para brindar un servicio, en el cual se podrá ofrecer la capacidad de personalizar aspectos como: Interfaz gráfica (logo de la organización, colores de letras y temas de los paneles), categorías de las preguntas, las preguntas específicas).

Para realizar cualquier tarea, el administrador debe loguearse en el sistema con sus credenciales en el panel de acceso de administración en 'http: //hostname/admin'. Tal como se muestra en la Figura 7. Pantalla de inicio de sesión del administrador.

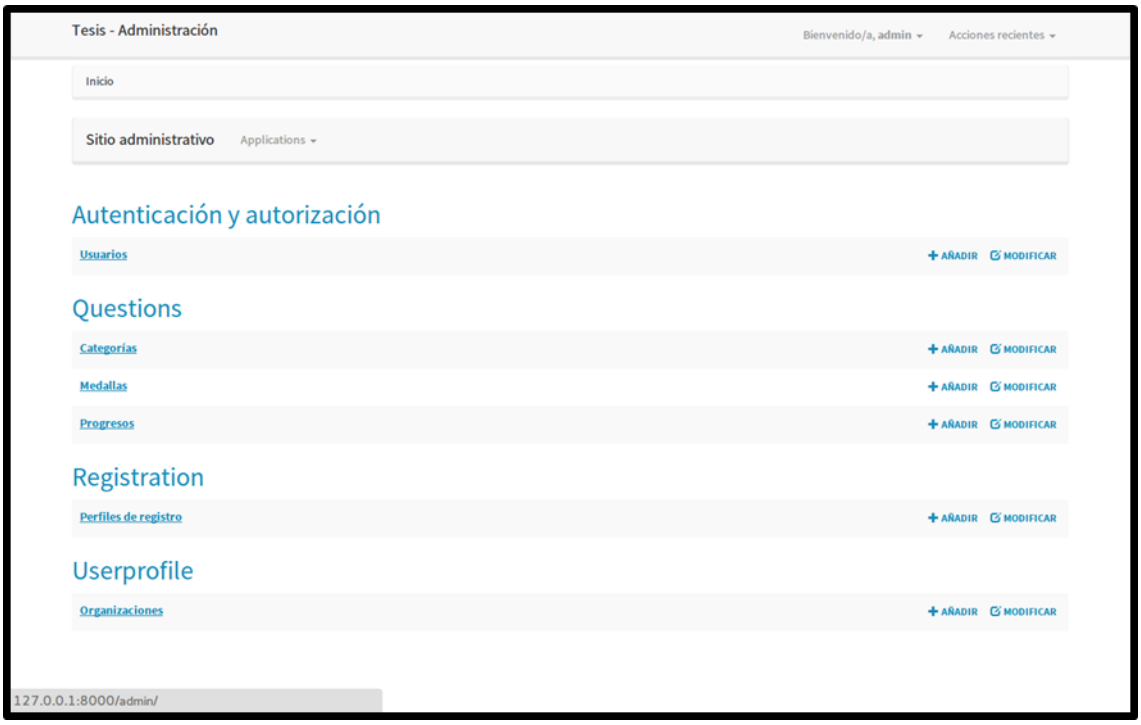
Figura 7. Pantalla de inicio de sesión del administrador.



Fuente: Elaboración propia.

Una vez el administrador ingrese al sistema, tiene a su disposición un menú que le permite gestionar las diferentes opciones de configuración de la aplicación, tal como se muestra en la Figura 8. Menú de Administración.

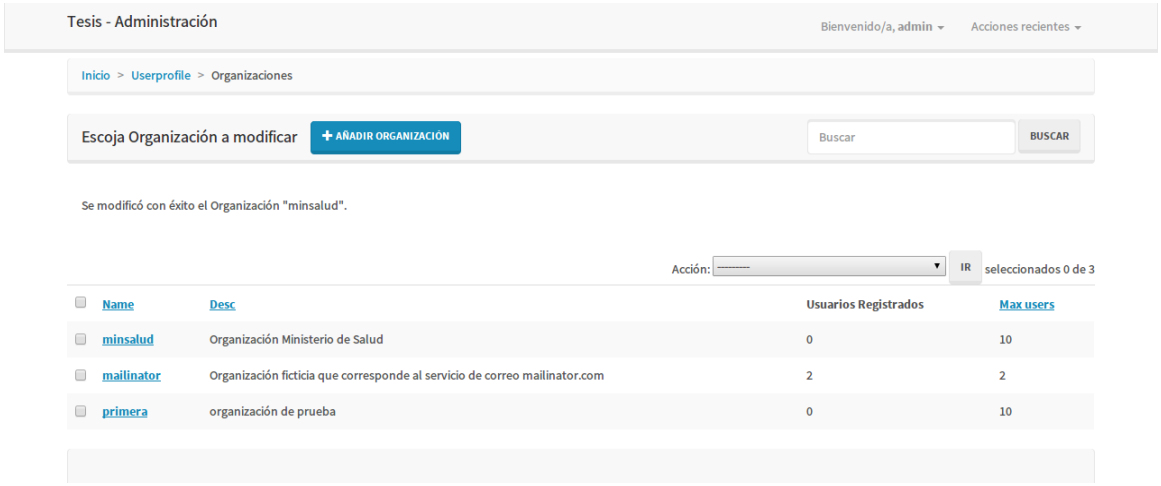
Figura 8. Menú de Administración.



Fuente: Elaboración propia.

5.1.1 Organizaciones. Para gestionar las organizaciones creadas en el sistema, el administrador debe ir al enlace 'Organizaciones', el cual le muestra una lista de las organizaciones creadas y diferentes opciones para crear o editar una organización, tal como se muestra en la Figura 9. Creación de organizaciones.

Figura 9. Creación de organizaciones.

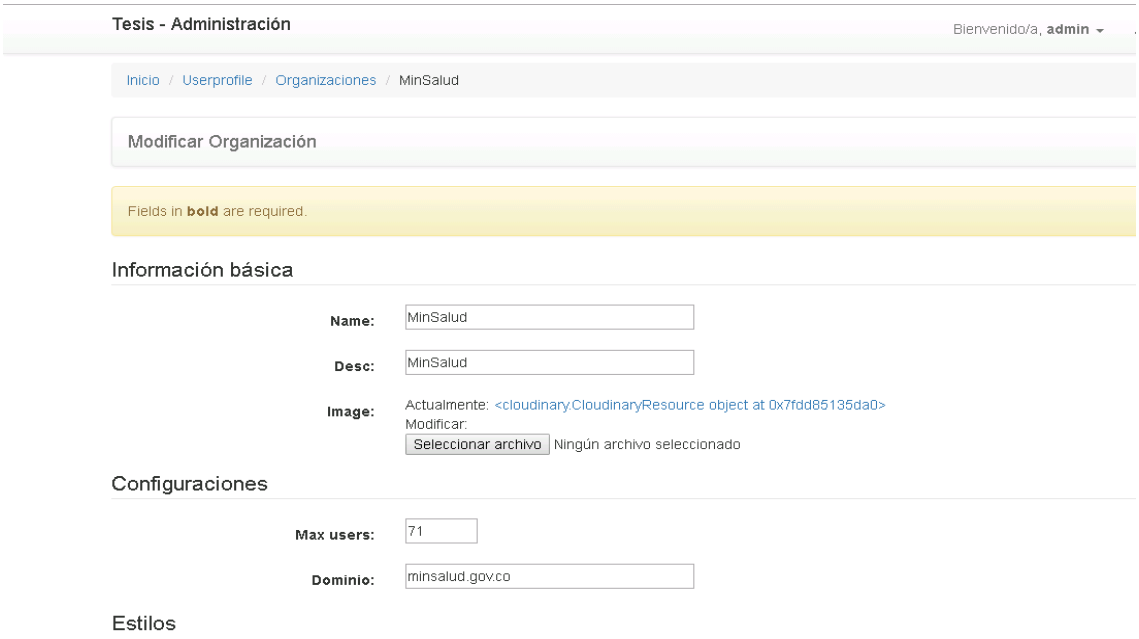


Fuente: Elaboración propia.

Si el administrador desea crear una organización puede hacerlo dando clic en el botón 'AÑADIR ORGANIZACIÓN' que aparece en el menú de las organizaciones. Esta opción le muestra al administrador una pantalla como la anterior con los diferentes campos en blanco para que se ingrese la información de la nueva organización.

Si el administrador desea editar una organización debe dar clic en el nombre de la organización y le aparecerá una pantalla con la información de la organización y la posibilidad de editar campos como descripción, imagen y número máximo de usuarios. En ésta pantalla también se muestran las opciones para personalizar los estilos gráficos de la aplicación según la organización. Lo anterior se puede en la Figura 10. Editar la información de una organización.

Figura 10. Editar la información de una organización.



Fuente: Elaboración propia.

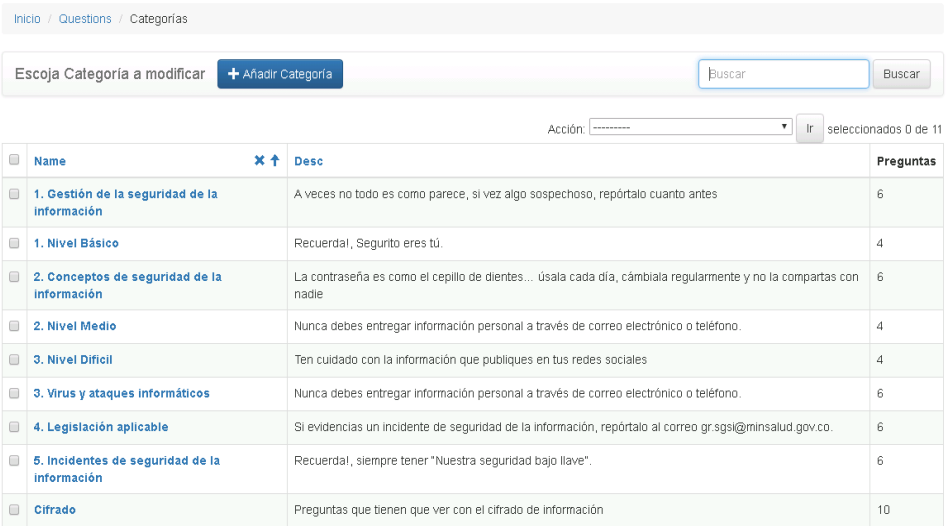
5.1.2 Categorías: Para gestionar las categorías el administrador debe dar clic en el enlace 'Categorías' del menú principal. Esto lo lleva al menú representado en la Figura 11. Gestionar categorías de preguntas, donde puede ver las diferentes categorías de preguntas que han sido creadas y que se encuentran disponibles actualmente en el sistema, así como también la descripción y el número de preguntas que cada una contiene.

Figura 11. Gestionar categorías de preguntas.

Fuente: Elaboración propia.

Si el administrador desea editar una categoría existente debe dar clic en el nombre de la categoría y se despliegan los campos: nombre, imagen, descripción y la lista de organizaciones a las cuales la categoría está asignada. En la Figura 12. Editar una categoría, se puede observar la interfaz gráfica.

Figura 12. Editar una categoría

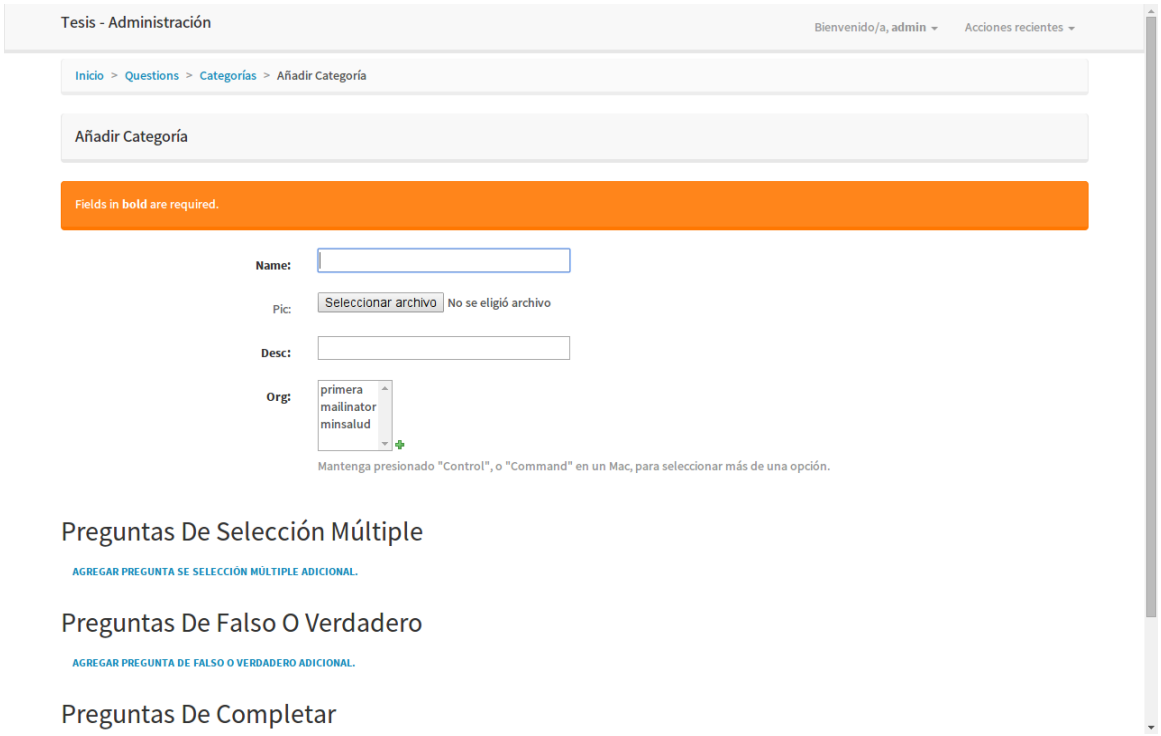


Fuente: Elaboración propia.

En esta misma pantalla el administrador puede gestionar las preguntas de la categoría y tiene la posibilidad de modificarlas, agregar nuevas o eliminar las existentes.

Para crear una nueva categoría el administrador debe dar clic en el botón 'AÑADIR CATEGORÍA' del menú de categorías, esto lo lleva a un formulario donde puede ingresar toda la información necesaria de la nueva categoría. El administrador debe asignar un nombre, una descripción y asociarla a una o más organizaciones creadas en el sistema, tal como se muestra en la Figura 13. Crear una nueva categoría.

Figura 13. Crear una nueva categoría.



Fuente: Elaboración propia.

5.1.3 Preguntas. Existen diferentes tipos de preguntas se despliega un formulario específico el cual puede requerir diferentes datos dependiendo del tipo de pregunta creada. La gestión de las preguntas se realiza en la misma página de las categorías.

Para las preguntas de tipo “completar” el formulario de requiere un campo con el texto de la pregunta. En el texto que se desea que el usuario identifique la palabra

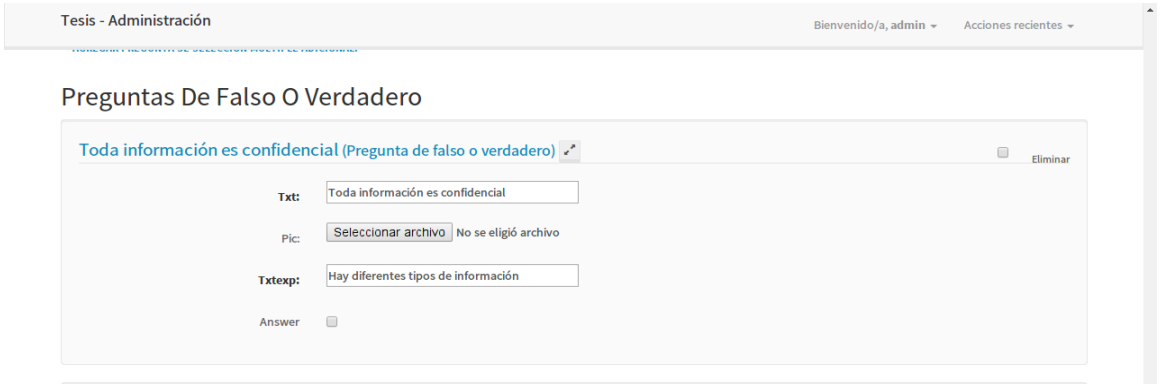
faltante, es necesario que se reemplace la palabra que el usuario deberá completar por un guion bajo '_'. La pregunta puede tener una imagen y debe tener un texto explicativo y una respuesta, la cual debe ingresar el usuario para completar la frase. Tal como lo muestra la Figura 14. Creación pregunta de tipo completar.

Figura 14. Creación pregunta de tipo completar.

Fuente: Elaboración propia.

Las preguntas de tipo falso o verdadero requieren la pregunta, el texto explicativo de la respuesta, y la respuesta, la cual se configura utilizando un 'checkbox', si este está seleccionado la respuesta es verdadera y si no lo está es falsa. La pregunta también puede tener una imagen asociada, tal como lo muestra la Figura 15. Creación Pregunta de Tipo Falso o Verdadero.

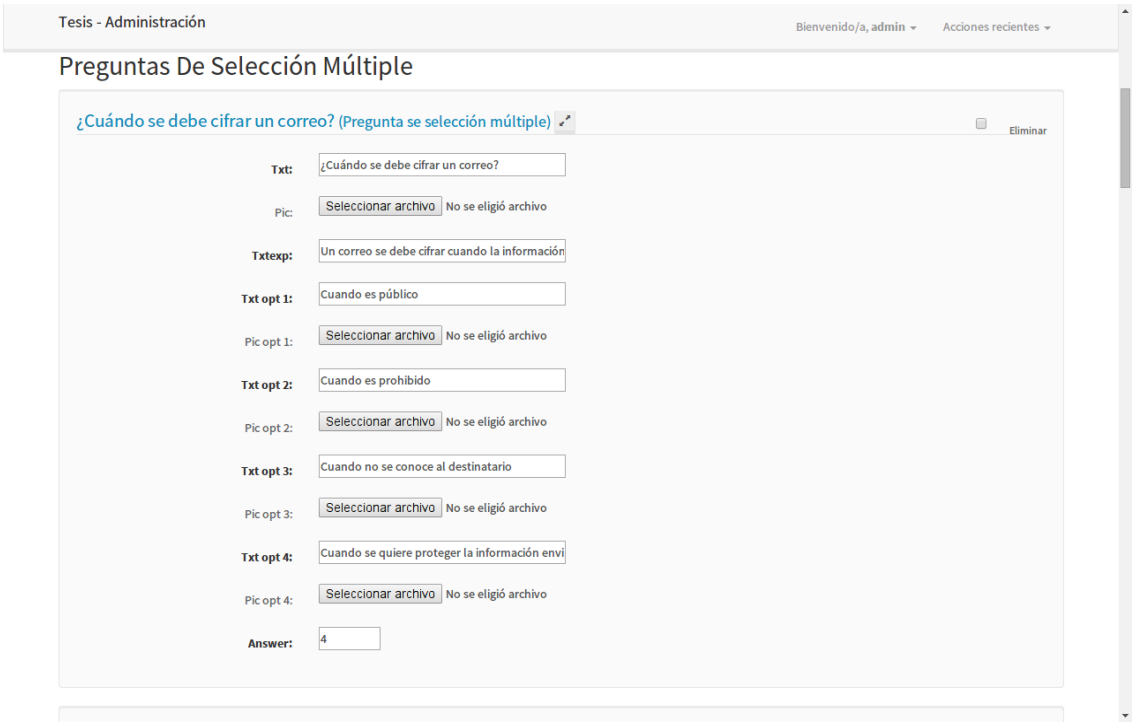
Figura 15. Creación Pregunta de Tipo Falso o Verdadero.



Fuente: Elaboración propia.

Las preguntas de selección múltiple deben tener un texto referente al enunciado de la pregunta, un texto explicativo y las 4 opciones de respuesta, se debe indicar cuál de las cuatro opciones es la respuesta correcta. Tanto el enunciado de la pregunta como las diferentes opciones pueden tener una imagen asociada, lo anterior se muestra en la Figura 16. Creación Pregunta de Tipo Selección Múltiple.

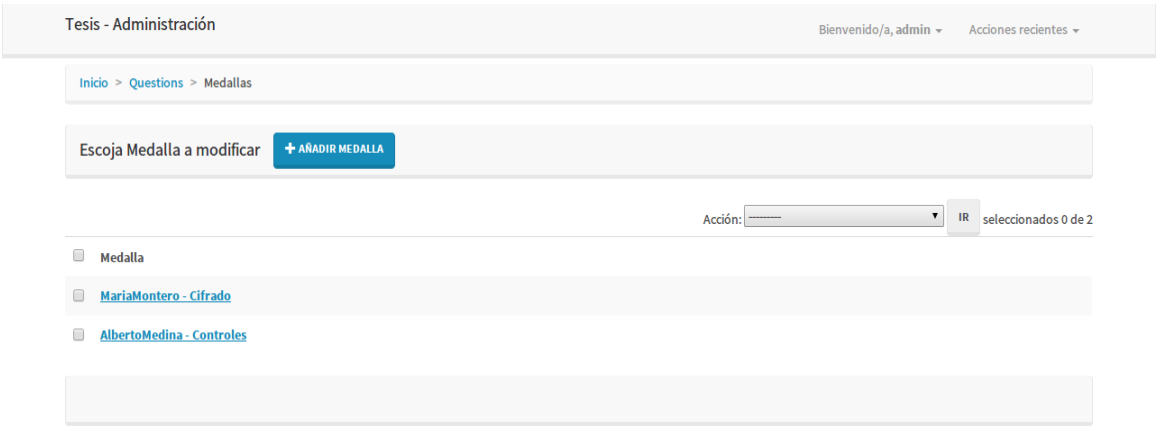
Figura 16. Creación Pregunta de Tipo Selección Múltiple.



Fuente: Elaboración propia.

5.1.4 Medallas. Las medallas hacen referencia a los logros alcanzados por un usuario al responder el total de preguntas de una categoría. Si el administrador desea ver las diferentes medallas que tienen los usuarios del sistema debe dar clic en el enlace 'Medallas' del menú principal. En la Figura 17. Administración de Medallas, se muestra la lista de medallas que relacionan los diferentes usuarios con las categorías que han completado. Esta lista de medallas se crea de forma automática a medida que los usuarios van completando las diferentes categorías y se organiza de forma cronológica de tal manera que permite saber qué usuario completó primero una categoría.

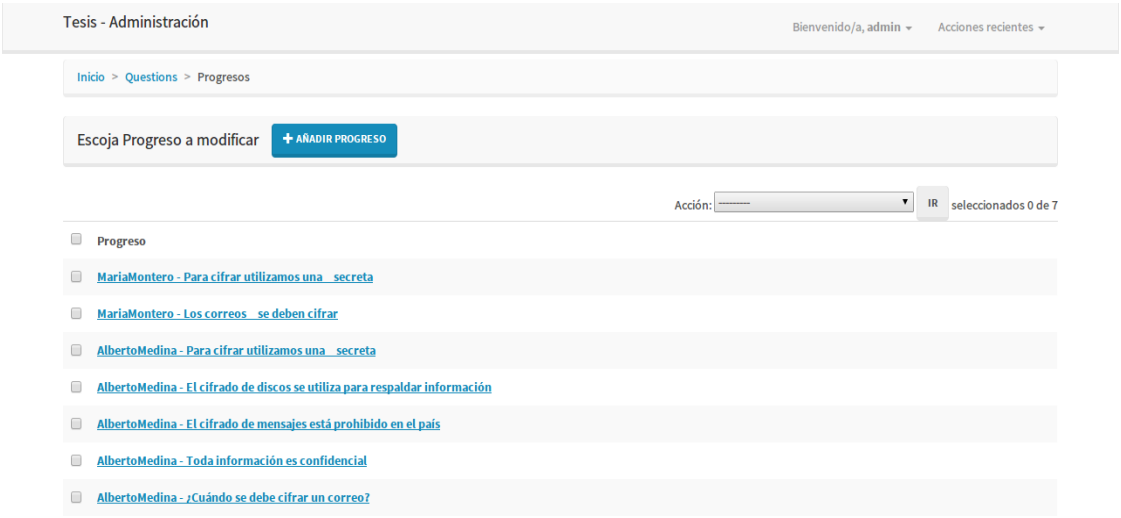
Figura 17. Administración de Medallas.



Fuente: Elaboración propia.

5.1.5 Progresos. Los progresos hacen referencia a la cantidad de preguntas que un usuario ha contestado correctamente sin haber terminado la categoría. Si el administrador desea ver los progresos de los diferentes usuarios del sistema debe dar clic en el enlace 'Progresos' del menú principal. En la figura 18. Administración del progreso de un usuario por categoría, se muestra la lista de progresos que relaciona los diferentes usuarios con las preguntas que ha respondido correctamente. Esta lista de preguntas contestadas se crea de forma automática a medida que los usuarios van contestando las preguntas y también se organiza de forma cronológica.

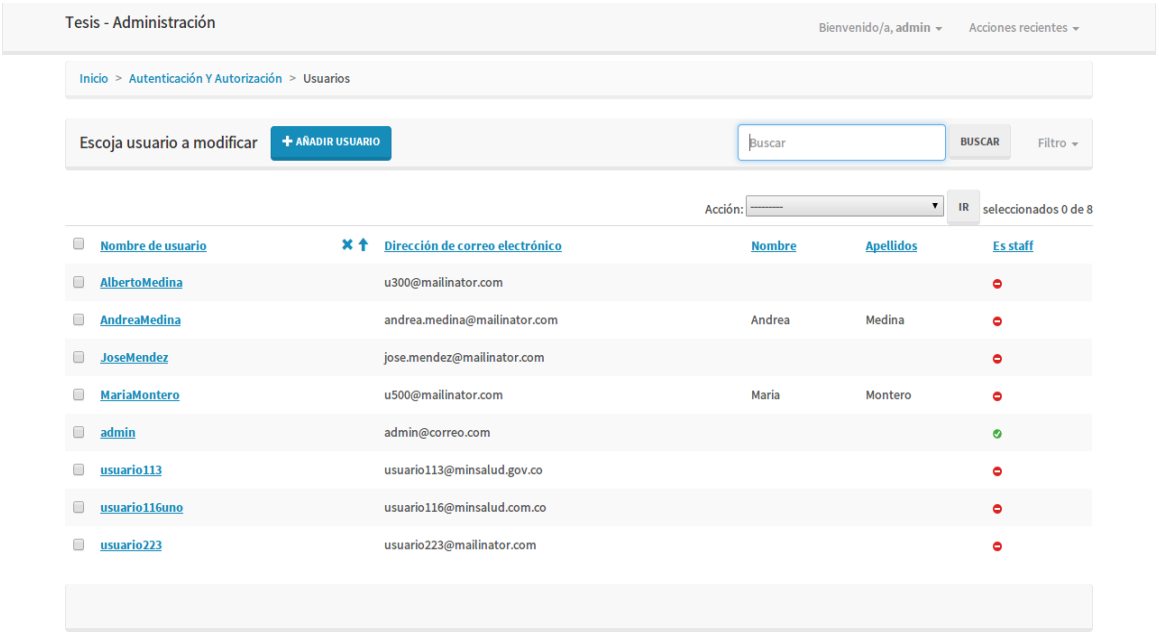
Figura 18. Administración del Progreso de un Usuario por Categoría.



Fuente: Elaboración propia.

5.1.6 Editar usuarios. El administrador podrá gestionar los usuarios del sistema dando clic en el enlace 'Usuarios' del menú principal, allí verá una lista de todos los usuarios del sistema y su información básica. Si se da clic en el nombre de algún usuario se va a una pantalla que permite editar la información del usuario, lo anterior se muestra en la Figura 19. Editar usuarios.

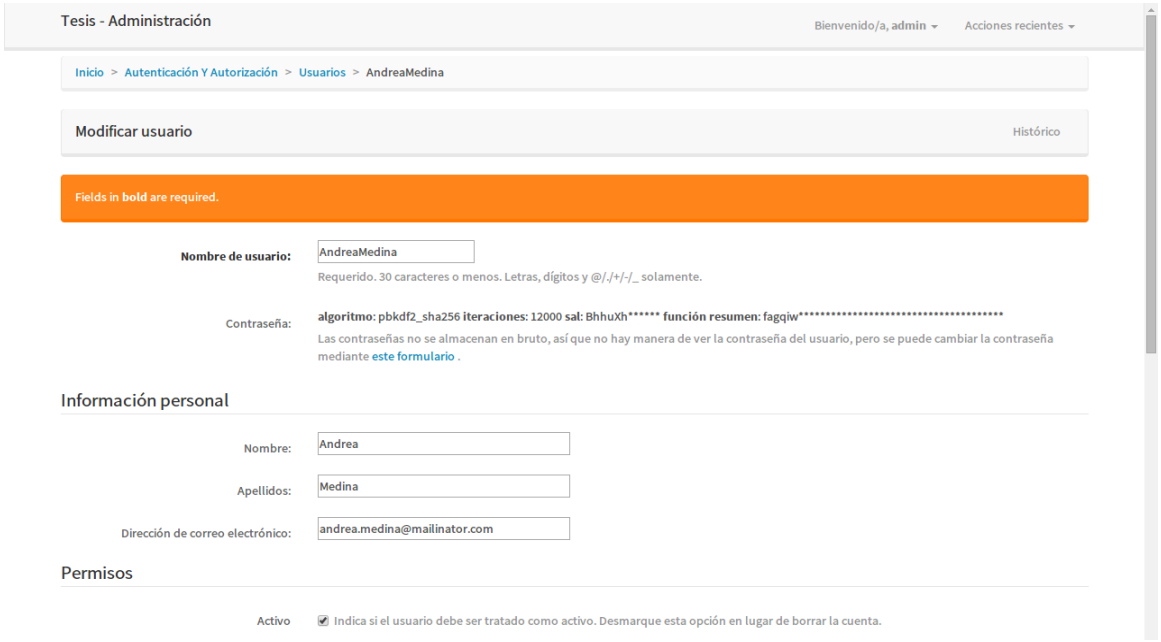
Figura 19. Editar Usuarios.



Fuente: Elaboración propia.

El administrador también puede ver el estado de registro de cada uno de los usuarios dando clic en el enlace 'Perfiles de registro' en el menú principal y si se requiere editar los datos del registro tal como se puede ver en la Figura 20. Edición/Registro de un usuario desde interfaz de administración.

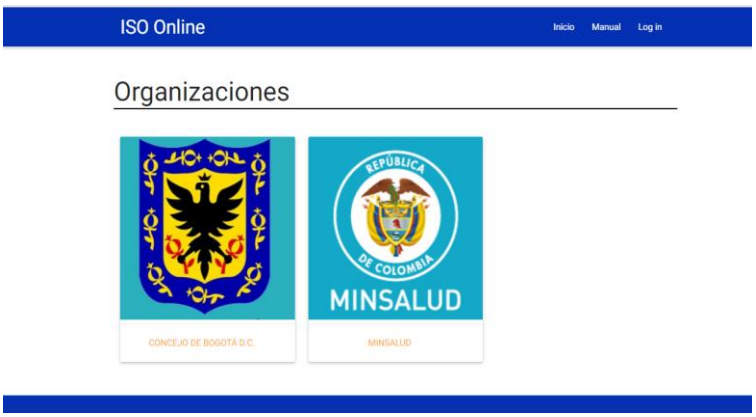
Figura 20. Edición/Registro de un Usuario desde Interfaz de Administración.



Fuente: Elaboración propia.

5.1.7 Página de inicio. Cuando el usuario ingresa en la aplicación es recibido por una pantalla en la que se le muestra un mosaico con los logos de las organizaciones disponibles, esto con el fin de que el Usuario, identifique y dé clic sobre el logo de su organización, tal como se muestra en la Figura 21. Página de inicio.

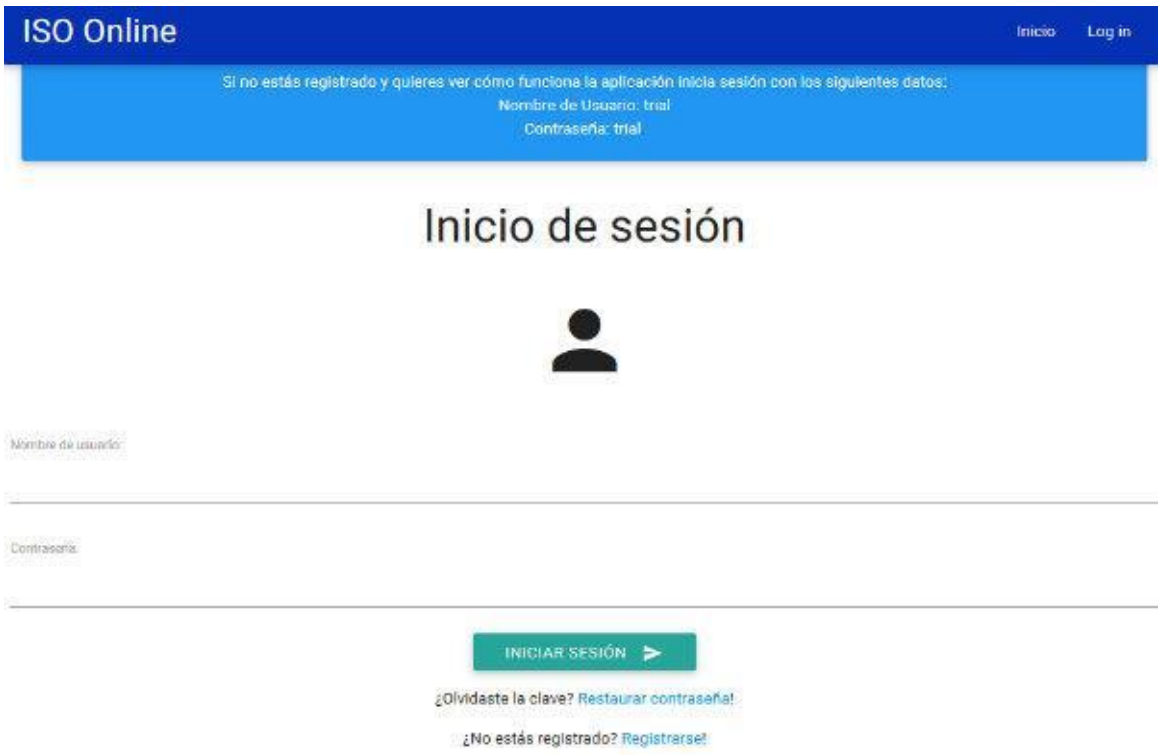
Figura 21. Página de inicio.



Fuente: Elaboración propia.

5.1.8 Inicio de sesión. Si el usuario ya tiene una cuenta activa en el sistema puede iniciar sesión dando clic en el enlace 'Log in' (Ver Figura 22. Inicio de sesión), esto lo llevará a una pantalla donde puede ingresar los datos de acceso. Si la información es correcta el usuario inicia sesión en el sistema y es dirigido a su página de perfil.

Figura 22. Inicio de Sesión.



Fuente: Elaboración propia.

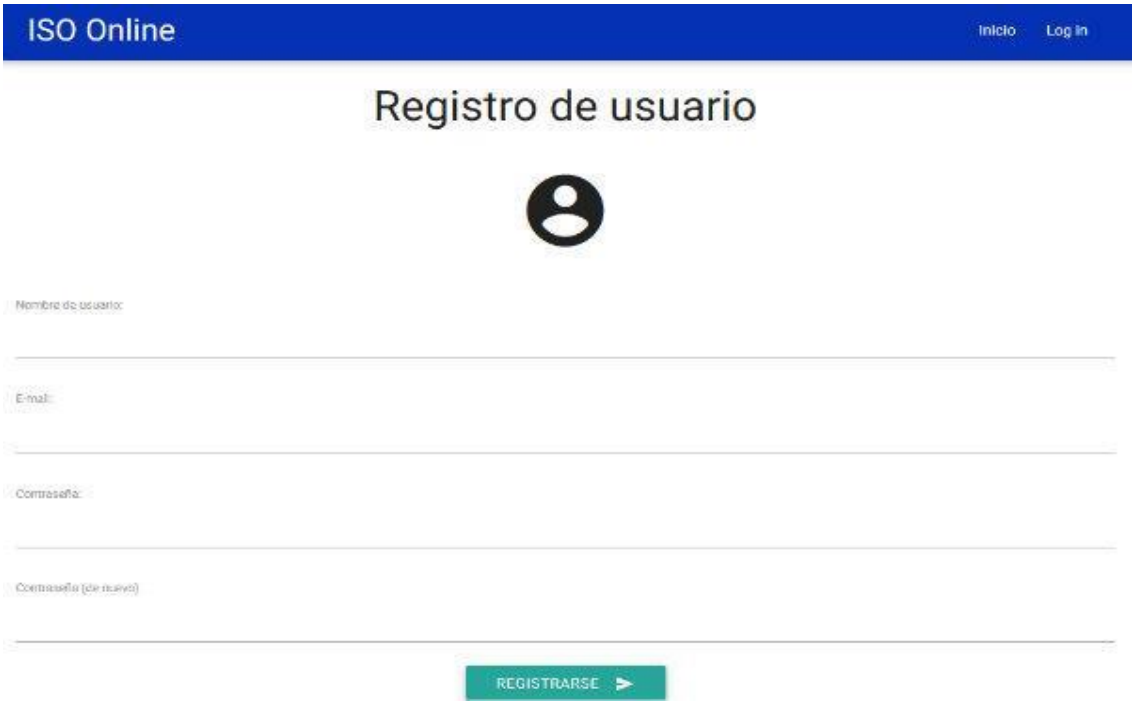
En caso de que el usuario haya olvidado su contraseña, puede dar clic en el enlace 'Restaurar Contraseña', el sistema le pedirá el correo electrónico al usuario y le enviará un mensaje con un enlace a través del cual puede volver a establecer una contraseña segura.

5.2 USUARIO

El usuario es quien hace uso de la herramienta web, para lo cual debe tener una cuenta activa. Si el usuario no tiene aún una cuenta debe dar clic en el enlace 'Registrarse', luego podrá ingresar los datos de registro. En este paso el sistema se encarga de validar que el correo electrónico proporcionado por el usuario corresponda a una organización creada en el sistema y que además no se haya alcanzado el número máximo de usuarios para la organización, si no se dan estas condiciones el proceso de registro no se puede llevar a cabo y se le notifica al usuario con un mensaje de error.

Existe un tipo particular de usuario llamado “usuario tester”, el cual en caso de no tener una cuenta activa, puede acceder a un número limitado preguntas de prueba.

Figura 23. Registro de Usuario Interfaz 1.



Fuente: Elaboración propia.

Figura 24. Registro de Usuario Interfaz 2.

Fuente: Elaboración propia.

Si el usuario no establece una imagen de perfil se utiliza la imagen de usuario por defecto de la aplicación.

Las características antes mencionadas se pueden evidenciar en la figura 23. Registro usuario interfaz 1 y figura 24. Registro de usuario interfaz 2.

5.2.1 Perfil de usuario. Cuando un usuario termina su proceso de registro e inicia sesión, es llevado a su página de perfil. En esta página se muestra en la parte superior el nombre de la organización a la cual el usuario pertenece y la imagen de la misma, también tiene enlaces para ir a la página de inicio y si da clic en su nombre de usuario se le muestra un menú con las opciones para ir a la página de perfil o cerrar sesión.

En el contenido de esta página se encuentran dos secciones, las dos secciones se encuentran representadas en la Figura 25. Perfil de usuario, en la primera se muestra la información del usuario, su nombre y apellido, nombre de usuario, puntos

acumulados y nombre de la organización a la que pertenece, también tiene un enlace para editar la información de perfil incluyendo la opción de modificar su contraseña, en la parte inferior de esta sección se muestran las diferentes categorías de preguntas que puede responder el usuario con una barra de progreso que muestra el avance del usuario en cada categoría. Si el usuario ya ha completado una categoría la barra de progreso aparece totalmente llena y al lado derecho del nombre de la categoría aparecerá una medalla que indica que la categoría ha sido completada.
La segunda sección se encuentra en el lado derecho de la pantalla y allí se muestra en ranking de usuarios de la organización. Se muestran los usuarios con mayor puntaje, sus nombres, puntos e imagen de perfil.

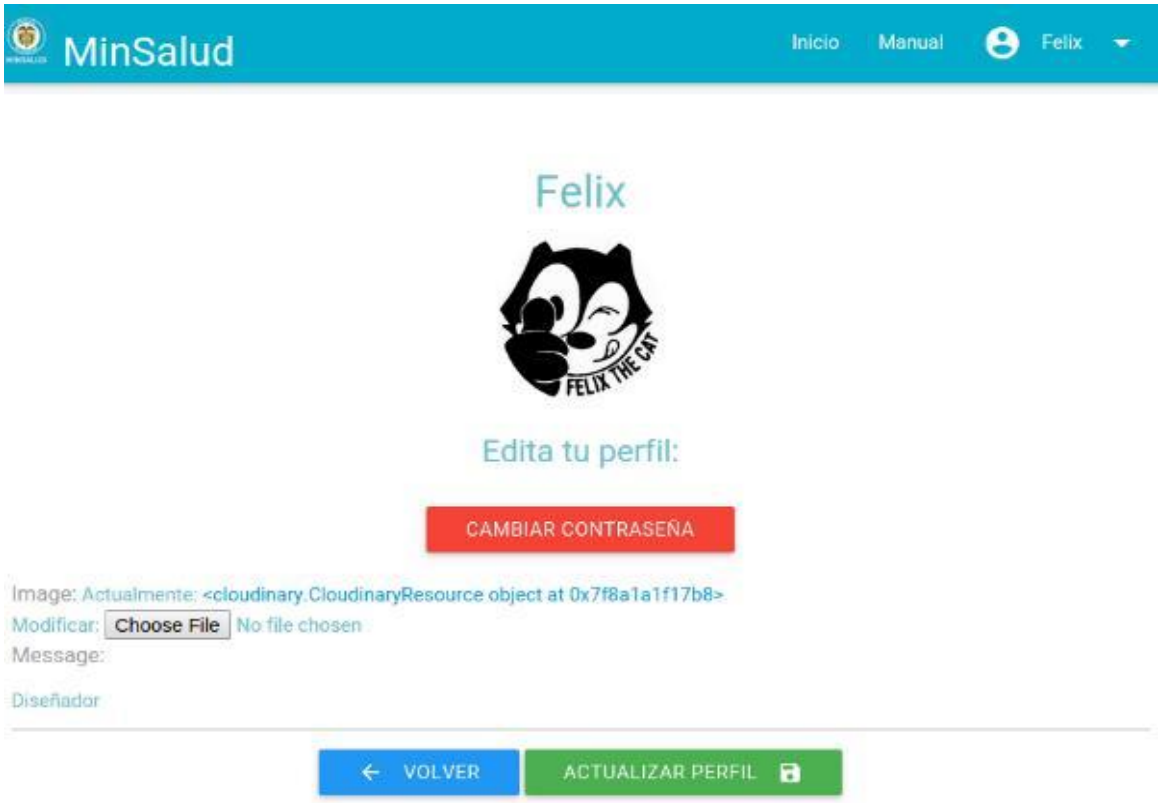
Si el usuario desea contestar preguntas de alguna categoría basta con darle clic al nombre de la categoría siempre y cuando la categoría no haya sido completada.

Figura 25. Perfil de Usuario.

Fuente: Elaboración propia.

5.2.2 Editar perfil. Si el usuario desea editar la información de su perfil puede dar clic en el enlace 'EDITAR PERFIL' que aparece junto a su información personal (ver Figura 25. Perfil de usuario), el cual presenta una pantalla, idéntica a la mostrada en la Figura 26. Editar Perfil, donde puede modificar su información personal, cambiar su contraseña y su imagen personal.

Figura 26. Editar Perfil.



Fuente: Elaboración propia.

5.2.3 Contestar preguntas. Cuando el usuario selecciona una de las categorías que todavía no ha completado, se presenta la página de responder preguntas, de acuerdo con lo ejemplificado en la Figura 27.Contestar pregunta – selección múltiple; en esta página se muestran dos secciones, una sección con el nombre, imagen y descripción de la categoría escogida y otra sección con el contenido de la pregunta y dos botones, uno rojo para regresar a la página de perfil sin responder la pregunta y otro verde para calificar la pregunta y continuar respondiendo otra.

Las preguntas se presentan al usuario según el tipo, las de selección múltiple muestra el enunciado junto con la lista de opciones de las cuales el usuario debe escoger la correcta, como se muestra en la imagen anterior. La secuencia y tipos de pregunta se pueden ver en la figura 27. Contestar pregunta - selección múltiple, figura 28. Contestar pregunta - falso o verdadero, figura 29. Contestar pregunta - completar palabra y figura 30. Respuesta correcta.

Figura 27. Contestar Pregunta - Selección Múltiple.

Fuente: Elaboración propia.

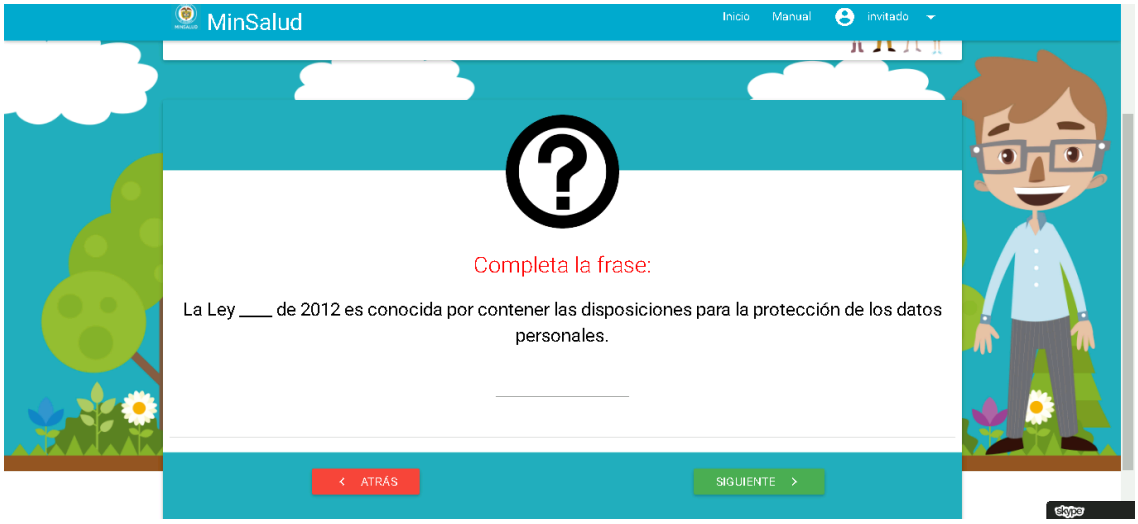
Las preguntas de falso o verdadero muestran el enunciado de la pregunta junto con un selector binario que permite escoger la respuesta como falso o verdadero.

Figura 28. Contestar Pregunta - Falso o Verdadero.

Fuente: Elaboración propia.

Las preguntas de completar muestran el enunciado, reemplazando las letras de la palabra que se debe completar por guiones bajos y con un campo de texto para que el usuario ingrese la respuesta que considere correcta.

Figura 29. Contestar Pregunta - Completar Palabra.



.

Fuente: Elaboración propia.

Cuando el usuario ingresa la respuesta a la pregunta que se le presenta y da clic en el botón verde, su respuesta es calificada por el sistema y se le muestra el resultado con una explicación.

Figura 30. Respuesta Correcta.

Fuente: Elaboración propia.

6. CONTENIDO DE LA HERRAMIENTA

Para crear el contenido de la herramienta web, orientada a generar impacto en el usuario, para adquirir compromiso, conciencia y cultura con la seguridad de la información, se busca un marco de referencia en cuanto a los estándares internacionales que aplican, recomendaciones, lineamientos, buenas prácticas y casos reales o noticias, el cual se presenta el Cuadro 3. Lista de Referencias para la creación de preguntas.

Cuadro 3. Lista de Referencias para la creación de preguntas.

Estándares Internacionales	**Recomendaciones / buenas practicas**	**Lineamientos / Normatividad**	**Noticias / casos reales**
Norma ISO[41] 27001:2013	ISACA[42] : Manual de Preparación al examen CISM 2015	Estrategia Gobierno en Línea	Portales de noticias Nacionales e internacionales
Norma ISO 31000:2011	ISACA : Manual de Preparación al examen CRISC 2015	Ley 1273 de 2009 "De la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	Portales web relacionados con seguridad informática y de la información
Norma ISO 27005:2008		Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"	

[41] http://www.iso.org/

[42] http://www.isaca.org/

Cuadro 3. (Continuación)

Estándares Internacionales	Recomendaciones / buenas practicas	Lineamientos / Normatividad	Noticias / casos reales
Norma ISO 27002:2013		Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales."	

Fuente: Elaboración propia.

El contenido se refleja en las preguntas presentadas en el presente capítulo, cada pregunta cuenta con la siguiente estructura:

- Pregunta
- Opciones de respuesta
- Respuesta y explicación

7. PRUEBA CAMPO DE LA APLICACIÓN

Para verificar la percepción de los usuarios finales, se realizó una prueba de campo a cien usuarios. La prueba se planeó con cinco categorías “Gestión de la seguridad de la información”, “conceptos de seguridad de la información”, “Virus y ataques informáticos”, “legislación aplicable”, “Incidentes de seguridad de la información”, cada una con un total de seis (6) preguntas.

7.1 PREGUNTAS USADAS DURANTE LA PRUEBA

7.1.1 Gestión de la seguridad de la información. En la categoría de Gestión de la Seguridad de la Información, se busca que el usuario final se relacione con los conceptos y directrices propias del SGSI.

- Pregunta

Le han hecho llegar para su firma una resolución que próximamente se publicará en la página web del Ministerio. Usted verifica si la información contenida es correcta. ¿Qué propiedad de la información está comprobando?

A. Disponibilidad
B. Exclusividad
C. Integridad
D. Integralidad

La Integridad es la propiedad que busca que los datos tengan exactitud, que no se hayan modificado indebidamente bien sea por usuarios autorizados o no autorizados, por lo cual al verificar que los datos sean correctos estas buscando validar la integridad de la información.

- Pregunta

¿Qué debes hacer si miras en las redes sociales que una persona publicó un enlace con alguna de las siguientes noticias: "Alerta de terremoto en Ecuador"; ¡Michael Jackson está vivo!; Romance entre Shakira y Alexis Sánchez?

A. Abrir el enlace, puede ser importante para estar informado.

B. Compartir la noticia con todos mis amigos o seguidores, así ellos estarán enterados.
C. Dejar un comentario en la publicación acerca de la falsedad de la noticia, ya que únicamente se utilizó para ganar popularidad.
D. No abrir el enlace y reportar la publicación inmediatamente, puede ser un método para propagar un virus informático.

Un ciberdelincuente logra (o intenta lograr) que su campaña de propagación de virus informáticos tenga éxito, aprovechándose de temáticas populares de actualidad. Las situaciones planteadas son ejemplos reales de noticias, personas y sucesos utilizados como gancho para captar víctimas.

- Pregunta

¿Cuál de los siguientes es uno de los tres pilares fundamentales de la seguridad de la información?

A. Disposición
B. Integralidad
C. Integridad
D. Confiabilidad

La integridad es una propiedad de seguridad de la información. ISO 27000 la define como “Propiedad de la información relativa a su exactitud y completitud”.

- Pregunta

¿Dónde se encuentra la documentación del Sistema de Gestión de Seguridad de la información?

A. En la página web del Ministerio.
B. En la intranet
C. Se obtiene mediante una solicitud al correo gr.sgsi@minsalud.gov.co
D. Se debe solicitar directamente a los servidores públicos de la OTIC.

Te invitamos a consultar en la Intranet el sitio del Sistema de Gestión de Seguridad de la Información.

- Pregunta

En el Ministerio de Salud y Protección Social, ¿Que significa la sigla “SGSI”?

A. Sistema de Gestión de Seguridad informática
B. Subsistema de Gestión de Seguridad informática
C. Subsistema de Gestión de la Información
D. Sistema de Gestión de Seguridad de la Información

El SGSI hace referencia al Sistema de Gestión de Seguridad de la Información.

- Pregunta

¿Qué debes hacer si te encuentras una memoria USB abandonada en el parqueadero, comedor, baños y en general otros sitios cercanos o al interior del Ministerio?

A. Conectar la memoria USB en tu computador, podrías encontrar indicios del propietario.
B. Pasar los archivos contenidos en la USB a tu computador y luego formatearla, así puede seguir utilizándola y al mismo tiempo resguardar la información.
C. Reportar el incidente, la memoria pudo haber sido dejada a propósito con fines malintencionados.
D. Compartirla con tus compañeros de oficina, de esta forma todos pueden almacenar su información de forma segura.

Ten cuidado, la memoria USB pudo haber sido utilizada para propagar un virus informáticos en el Ministerio. Esta técnica frecuentemente es utilizada por los ciberdelincuentes.

7.1.2 Conceptos de seguridad de la información. La categoría de conceptos de seguridad de la información, le da al usuario final un abrebocas sobre algunos conceptos teóricos necesarios para lograr un entendimiento de seguridad de la información, así como del SGSI y sus requerimientos.

- Pregunta

Suponiendo que cinco ingenieros pertenecientes al grupo de soporte informático, comparten una misma tarjeta de acceso al centro de datos. ¿Cuál es el mayor riesgo de seguridad de la información que conlleva esto?

A. Si la tarjeta de acceso se pierde, los cinco ingenieros no podrían ingresar.
B .Si se requiere ingresar a trabajar, se pierde tiempo al buscar a quien tenga la tarjeta de acceso en ese momento.
C. Si ocurre un incidente dentro del centro de datos, no estará claro quién es responsable.
D. Los ingenieros pueden compartir la tarjeta de acceso con otras personas.

Aunque las opciones A, B y D son consecuencias validas, no afectan la seguridad de la información. La respuesta correcta es la opción C, debido a que si se comparten la tarjeta de acceso, dificulta el registro y control de ingreso, al igual que la investigación en caso de incidentes de seguridad de la información.

- Pregunta

¿En qué casos no se recomienda hacer uso de la nube, como Google Drive o Dropbox?

A. Para compartir la información pública con otras personas.
B. Para almacenar información clasificada y/o reservada a modo de copia de seguridad
C. Para guardar documentos descargados de internet.
D. Para almacenar mi música favorita.

No es recomendable almacenar en la nube información clasificada y/o reservada, generalmente la “nube” tiene sus servidores en otro país, por lo que se puede desconocer la regulación legal aplicable a dicho almacenamiento.

- Pregunta

Es recomendable tener anotadas las contraseñas en algún lugar, de esta forma, si se nos olvida, podemos consultarlas rápidamente.

A. Estoy de acuerdo
B. Estoy de acuerdo solo si la contraseña es robusta
C. No es recomendable

D. Estoy de acuerdo solo si la cambias todos los días

La contraseña es algo privado, no es recomendable dejarla escrita en ningún sitio, y mucho menos al lado del computador. Personas inescrupulosas pueden acceder sin ser autorizadas a su información o robar su identidad.

- Pregunta

¿Qué debes hacer si te llega un correo de procedencia sospechosa, invitándote a enviar tus datos personales o a dar clic en un enlace a cambio de un regalo?

A. Eliminarlo inmediatamente
B. No abrirlo y reportar el evento inmediatamente
C. Abrirlo y comprobar de que se trata el correo
D. Reenviarlo a tus compañeros para que entre todos verifiquen el contenido.

Si te llega un correo sospechoso no debes abrirlo y repórtalo inmediatamente, si se comprueba que es un correo malicioso, se bloqueará la dirección de e-mail del remitente para que ningún servidor público del Ministerio sea víctima de fraude.

- Pregunta

La ingeniería social es…

A. Un virus
B. Técnica utilizada para sustraer información a otras personas teniendo como base la Interacción social.
C. Una carrera universitaria complementaria a la Seguridad Informática
D. Una campaña de sensibilización en seguridad de la información

Según se expone en la revista enter.co, la ingeniería social es una técnica de hackeo utilizada para sustraer información a otras personas teniendo como base la interacción social.

- Pregunta

Teniendo en cuenta la política del sistema de gestión de seguridad de la información, publicada en la intranet, se puede inferir que su cumplimiento se RESTRINGE a?

A. La Oficina de Tecnología de la Información y la Comunicación, OTIC
B. Todo el Ministerio
C. Únicamente los funcionarios de carrera del Ministerio, exceptuando a los contratistas.
D. Únicamente para las personas que la conozcan

Todos los servidores públicos del Ministerio deben conocer y apoyar el cumplimiento de la política del sistema de gestión de seguridad de la información.

7.1.3 Virus y ataques informáticos. En esta categoría se brida al usuario final, conciencia sobre seguridad informática y conceptos de los mismos que más adelante pueden contribuir a la identificación de un incidente y a tomar precauciones al usar sus estaciones de trabajo.

- Pregunta

Analice la siguiente afirmación: los únicos sistemas operativos que no se ven afectados por virus son los Mac OS de Apple, por eso los fabricantes de antivirus no desarrollan herramientas de seguridad para los dispositivos de esta marca.

A. Estoy de acuerdo.
B. Los virus solo afectan a los equipos con sistema operativo Windows.
C. A pesar de que existen virus para los Mac OS de Apple, no existen antivirus para este sistema operativo.
D. Todos los sistemas operativos están expuesto a los virus informáticos.

Es un falso mito. Si bien es cierto que la mayoría de virus son desarrollados para afectar a dispositivos Windows, los virus también afectan a los sistemas operativos Mac OS de Apple o Linux.

- Pregunta

¿Cuál de los siguientes software se puede considerar malicioso?

A. Correo electrónico.
B. Antivirus
C. Anti-spam

D. Malware

El malware (del inglés “malicious software”), es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

- Pregunta

¿Cuantos programas antivirus es recomendable tener instalado en su computador, portátil o dispositivo móvil?

A. Lo recomendable es tener dos (2) antivirus instalados
B. Con un solo antivirus es suficiente siempre y cuando esté actualizado
C. Cuantos más programas antivirus tengas instalados en el computador, mejor. Menos virus se colarán en él
D. Lo recomendable es tener tres (3) antivirus instalados

Lo importante para detectar los nuevos virus es que el antivirus se encuentre actualizado, por el contrario si dos o más antivirus trabajan a la vez en un mismo computador es muy probable que genere conflictos afectando el rendimiento del computador.

- Pregunta

¿Qué es el Phishing en seguridad de la información?

A. Es la recolección de contraseñas a través de un virus informático.
B. Es un correo electrónico enviado masivamente con copia oculta (CCO)
C. Es un sitio web suplantado o duplicado para engañar a quien lo visite
D. Es la capacidad para modificar el contenido de un sitio web.

Un ataque tipo Phishing consiste en intentar adquirir información mediante la suplantación de una persona o empresa de confianza en una aparente comunicación oficial.

- Pregunta

En seguridad de la información ¿En qué consiste un ataque de diccionario?

A. Utilizar el diccionario para buscar definiciones y métodos para afectar la seguridad de la información
B. Intentar averiguar una contraseña probando todas las palabras del diccionario
C. Utilizar palabras de otros idiomas para crear contraseñas seguras
D. Golpear los equipos de cómputo accidentalmente con un diccionario

El ataque de diccionario es utilizado por los ciberdelicuentes ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña, para que sea fácil de recordar, lo cual no es una práctica recomendable. Los ataques de diccionario tienen pocas probabilidades de éxito con contraseñas fuertes, con letras en mayúsculas y minúsculas mezcladas con números y símbolos.

- Pregunta

Tener un antivirus instalado es la única forma de proteger la información de todas las amenazas que circulan por Internet.

¿Falso o verdadero?

Tener instalado un antivirus en sus dispositivos es muy importante, sin embargo, como una única medida de seguridad no es suficiente, el antivirus debe ir acompañado de buenas prácticas de seguridad.

7.1.4 Legislación aplicable. Las preguntas contenidas en esta categoría hacen referencia a todas aquellas leyes, normas, o directrices que aplican al SGSI y a la entidad en general y que están relacionadas con seguridad de la información.

- Pregunta

¿Es un delito conectarse a una red WiFi sin autorización expresa del propietario, aunque sólo sea para visitar alguna página web, consultar perfiles de redes sociales o leer el correo electrónico?

A. En ningún caso es un delito.
B. Correcto, es un delito.
C. Es un delito únicamente si se descargan películas, música o software pirata.
D. No es un delito si solo se utiliza para navegar en páginas web seguras.

El acceso a un sistema de información de forma no autorizada, incluyendo una red WiFi, es un delito según la ley 1273 DE 2009 conocida como "De la protección de la información y de los datos".

- Pregunta

La Ley conocida como "de transparencias y del derecho de acceso a la información pública" es la:

A. Ley 1581 de 2012
B. Ley 1273 de 2009
C. Ley 23 de 1982
D. Ley 1712 de 2014

El objeto de la Ley 1712 de 2014 es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

- Pregunta

¿Cuál es la Norma Técnica Colombiana (NTC-ISO-IEC) elaborada para suministrar requisitos para el establecimiento, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información?

A. 9001
B. 27001
C. 31000
D. 14000

El Sistema de Gestión de Seguridad de la Información del Ministerio se está implementando teniendo en cuenta los requisitos de la norma NTC-ISO-IEC 27001 en su versión 2013.

- Pregunta

¿Cuál es el lema de la seguridad de la información del Ministerio?

A. "Es por nuestra seguridad"
B. "Nuestra seguridad bajo llave".

C. “Seamos pilosos con la seguridad”
D. “Todo por la seguridad”

Recuerda mantener “nuestra seguridad bajo llave”.

- Pregunta

¿Cuál de los siguientes enunciados NO se encuentra en el decálogo de la seguridad de la información del Ministerio?

A. Bloquee la sesión de su equipo de cómputo cada vez que se ausente de su puesto de trabajo.
B. La contraseña es como el cepillo de dientes… úsala cada día, cámbiala regularmente y no la compartas con nadie.
C. No instale software no autorizado o pirata en los equipos de cómputo. Siempre utilice software licenciado.
D. Evite almacenar sus contraseñas en lugares visibles y compartirlas con otros usuarios.

Te invitamos a consultar en la intranet el decálogo de la seguridad de la información.

- Pregunta

La Ley de 1581 de 2012 es conocida por contener las disposiciones para la protección de los datos personales.

¿Falso o verdadero?

La Ley de 1581 de 2012, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

7.1.5 incidentes de seguridad de la información

Las preguntas relacionadas en esta categoría, pretenden sensibilizar y enseñar a identificar y reportar incidentes de seguridad de la información, así como a generar conciencia sobre las consecuencias de los mismos.

- Pregunta

¿Cuál de los siguientes ejemplos, constituye un incidente que afecta la confidencialidad de la información?

A. La página web no se encuentra disponible
B. Borrar datos accidentalmente
C. Usar información del Ministerio para fines particulares.
D. Falsificar firmas.

Al usar la información del Ministerio con fines particulares, afectamos la confidencialidad de la información clasificada y reservada.

- Pregunta

En la noticia publicada en Colombia: Correo electrónico del presidente Santos fue 'chuzado', en la cual, se expresa que los mensajes privados del mandatario y de su familia fueron interceptados por desconocidos. ¿Qué pilar de la seguridad de la información se afectó?

A. Integridad
B. Confidencialidad
C. Disponibilidad
D. Confianza

Dicha noticia fue publicada por el periódico el tiempo el 22 de febrero de 2014. Según la norma ISO 27001, la confidencialidad es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Pregunta

En el Ministerio se reportan los siguientes eventos: evento 1: se extravió documentación del archivo central; evento 2: alguien accede a un correo electrónico de un compañero sin ser autorizado; evento 3: la pantalla de mi equipo está fallando y no me permite visualizar imágenes en alta definición. ¿Cuál de estos eventos NO es un incidente de seguridad de la información?

A. Evento 1
B. Evento 2
C. Evento 3
D. Todos los eventos se consideran incidentes de seguridad de la información.

El evento 3 no afecta la seguridad de la información y debe ser reportado únicamente a la mesa de ayuda. Los eventos 1 y 2 se consideran incidentes que pueden afectar la confidencialidad, integridad o disponibilidad de la información.

- Pregunta

El correo electrónico donde se deben reportar los incidentes de seguridad de la información es:

A. comunicaciones@minsalud.gov.co
B. sgsi@minsalud.gov.co
C. soporteune@minsalud.gov.co
D. gr.sgsi@minsalud.gov.co

Reporta los eventos e incidentes de seguridad de la información al correo gr.sgsi@minsalud.gov.co

- Pregunta

Un virus informático en el equipo de cómputo puede borrar o modificar archivos, e incluso inutilizar mi antivirus si este no está actualizado…

A. En ningún caso, los virus no pueden hace eso.
B. No exactamente, el antivirus nunca se puede inutilizar.
C. Si, esas son sus principales acciones
D. Los virus informáticos no existen.

Un virus informático es un malware que tiene por objetivo alterar el normal funcionamiento del computador, los virus pueden destruir los datos almacenados, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos. Es de anotar que si un antivirus no se encuentra actualizado, existe la probabilidad de que sea inutilizado o no detecte los nuevos virus.

- Pregunta

Analice la siguiente afirmación: conectarse a una red WiFi pública es peligroso sólo si se hace desde computadores de escritorio o portátiles, los Smartphone y tabletas no corren ningún riesgo.

A. Estoy de acuerdo.
B. Es falso, una red WiFi pública es segura para cualquier dispositivo.
C. La información de los Smartphone y tabletas también es vulnerable si estos dispositivos son conectados a redes desconocidas.
D. Una red WiFi pública es segura siempre y cuando se navegue de forma anónima.

Si un dispositivo es conectado a redes desconocidas, existe el riesgo de afectar la confidencialidad de la información, por esta razón nunca realices transacciones cuando estés conectado desde una red WiFi pública.

7.2 METODOLOGÍA USADA DURANTE LA PRUEBA

Para la realización de la prueba se realizó un concurso durante un día, la aplicación se puso en línea y se le dio acceso a las personas de 8 a.m. a 5 p.m. buscando que las personas pudieran realizan la activada en cualquier momento de su jornada laboral e incluso responder en tiempos no continuos. El concurso se denominó "¿CUANTO SABES SOBRE LA SEGURIDAD DE LA INFORMACIÓN?", en el cual, aprovechando los medios de difusión proporcionados y normalmente utilizados por el Ministerio de Salud y la Protección Social, se difundió por medio de la intranet a los colaboradores las reglas del concurso las cuales consistían en:

1. El servidor público debe ingresar a la página web desde el enlace entregado en el correo de invitación al concurso.

2. El Servidor público debe registrarse al concurso con su cuenta de correo electrónico.

3. Las categorías de las preguntas que se encontrarán son los siguientes:

- Nivel 1. Gestión de la Seguridad de la Información

- Nivel 2. Conceptos básicos de seguridad de la información
- Nivel 3. Virus y ataques informáticos
- Nivel 4: Legislación aplicable.
- Nivel 5. Incidentes de Seguridad de la Información

4. Cada categoría contendrá 10 preguntas sobre seguridad de la información. Cada usuario obtendrá una puntuación que dependerá de su desempeño al responder las preguntas. Por cada pregunta correcta se asigna 10 puntos, cada respuesta equivocada resta 5 puntos, si el usuario no tiene puntos no se restan, es decir, el mínimo número de puntos es 0.

5. El servidor público ganador será quien al final del quinto 5° nivel obtenga la mayor puntuación. En caso de empate, el ganador será quien haya contestado las preguntas en el menor tiempo.

7.3 RESULTADOS DE LA PRUEBA

El día 23 de noviembre de 2015 se dispuso la plataforma de concurso en la url: http://upiloto.isoonline.com.co/user/profile/ en la cual los servidores públicos del Ministerio de Salud y la Protección Social ingresaron y respondieron las preguntas planteadas teniendo la oportunidad de acumular puntos y crear un puntaje para posicionarse en la escala de puntajes. Posteriormente se indicaron los mayores puntajes conseguidos durante el desarrollo del juego, en la figura 31. Plataforma del concurso, se puede observar un ejemplo de la clasificación así como observar las categorías que los servidores públicos respondieron. Los puntajes obtenidos se muestran en el Cuadro 4. Mejores puntajes obtenidos.

Figura 31. Plataforma concurso.

Fuente: Elaboración propia.

Cuadro 4. Mejores puntajes obtenidos mediante la plataforma.

Nombre	Puntos
Julián Felipe Olarte Rueda	300 puntos
Alcira Velásquez Santiago	300 puntos
Wilson Duran Silva	300 puntos
María Luisa Fernanda Rodríguez Rivas	300 puntos
Yuli Janeth Ballén Pulido	300 puntos
María Lucen Ruiz Suarez	300 puntos
María Fernanda Del Pilar Solano Cruz	300 puntos
Andrés Felipe Meneses Segura	300 puntos
Marcela Mosquera Bernal	300 puntos
Ricardo Azaque	300 puntos
Fabiola Cruz Ureña	300 puntos
Adriana Carolina Rodríguez Cortes	300 puntos
Linda Johana Peña Hurtado	300 puntos
Jorge Alexander Guateque Martínez	295 puntos
Paola Vanegas	295 puntos
Andrea Johanna Lara Sánchez	290 puntos
John Alexander Rivera Becerra	290 puntos

Cuadro 4. (Continuación)

Nombre	Puntos
Tatiana Gaitán Linares	290 puntos
María Ruth Velasco	290 puntos
Javier Ricardo Bohórquez Gelvez	285 puntos
Jose Infante Garcia	285 puntos
Julio Cesar Ospina Marmolejo	285 puntos
Juliana Restrepo Hernández	285 puntos
Brigitte Neffer Forest Duque	280 puntos
Jarry James Rivera Lozano	280 puntos
María Alejandra Martínez Carrillo	280 puntos
Martha Lucía Ospina Gómez	280 puntos
Andrea Solis	275 puntos
Alexander Arévalo Sánchez	275 puntos
Catherine Ramírez Gutiérrez	275 puntos
Jose Luis Cuero León	275 puntos
Rodrigo Restrepo	275 puntos
Hernán Arroyo Benítez	270 puntos
Martha Espinel Mancera	270 puntos
Marcela Pilar Rojas Diaz	270 puntos
Ricardo Luque Núñez	270 puntos
Claudia Lizeth Godoy Moreno	265 puntos
Diana Yazmin Angarita Prada	265 puntos
Dwight Ospina Agredo	265 puntos
Johanna Mayorga Amador	265 puntos
Claudia Mayerly Duarte Torres	260 puntos
Ingrid Morales Cubillos	260 puntos
Jorge Daniel Solano Paz	260 puntos
Keila Saucedo Cadena	260 puntos
Robert Edward Turriago Romero	260 puntos
Sandra Liliana Silva Cordero	260 puntos
Smith Villamizar Arteaga	260 puntos
Yeimy Zulema Vargas Pineda	260 puntos
Alfonso Andrade Peña	255 puntos
Luisa Sabogal	255 puntos
Ramiro Augusto Moreno	255 puntos
Diego Fernando Arciniegas	250 puntos

Cuadro 4. (Continuación)

Nombre	Puntos
Carmen Julia Garcia Ballesteros	250 puntos
Dilsa Delith Riveros Diaz	250 puntos
Ronald Alexander Quintero Viasus	250 puntos
Schneider Mendieta B.	245 puntos
Astrid Berena Herrera López	235 puntos
Claudia Colorado	230 puntos
Carlos Mauro Vanegas Caviedes	220 puntos
Miguel Ángel García Ferro	215 puntos
Eliana Osorio Gonzalez	210 puntos
Patricia Caro Jiménez	210 puntos
Hernando Pérez Camelo	195 puntos
María Nina Zambrano Trujillo	190 puntos
Yeimi Yohana Alvarado Morales	190 puntos
Imelda De Las Mercedes Murcia	55 puntos
Karys Yaritza González Urrutia	55 puntos
Mary Isabel Patino Pinzon	35 puntos
Alvaro Enrique Alvarez Pardo	0 puntos
Amanda Valdes Soler	0 puntos
Diego Rene Torres Galindo	0 puntos
John Alexander Sánchez Bejarano	0 puntos
Luis Orlando Rodríguez Garzón	0 puntos
Claudia Lucía Morales Torres	0 puntos
Miguel Ángel Amaya Peñuela	0 puntos
Raúl Marcelino Herrera García	0 puntos
Sduran	0 puntos
Yuri Sonia Pachón Salazar	0 puntos

Fuente: Elaboración propia.

De la Tabla 1. Resumen de puntajes, se puede deducir que de las 78 personas evaluadas, 13 lograron obtener un puntaje perfecto de 300 Puntos mientras que las 10 personas restantes que se inscribieron y registraron en la plataforma pero no realizaron el test o no lograron puntaje.

Tabla 1. Resumen puntajes.

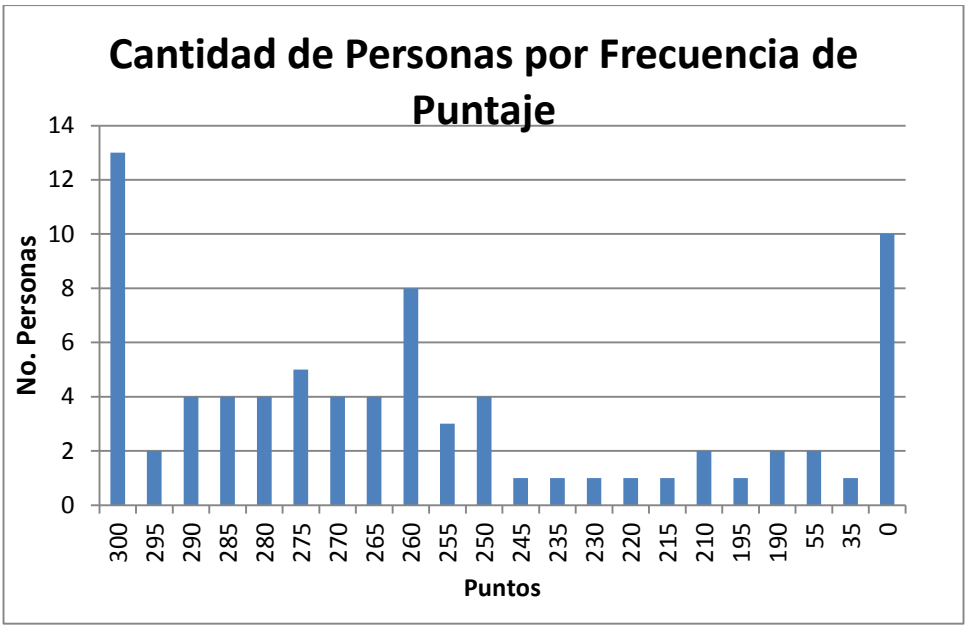
Puntaje	Número de personas
0 puntos	10
190 puntos	2
195 puntos	1
210 puntos	2
215 puntos	1
220 puntos	1
230 puntos	1
235 puntos	1
245 puntos	1
250 puntos	4
255 puntos	3
260 puntos	8
265 puntos	4
270 puntos	4
275 puntos	5
280 puntos	4
285 puntos	4
290 puntos	4
295 puntos	2
300 puntos	13
35 puntos	1
55 puntos	2

Fuente: Elaboración propia.

Durante el concurso las personas aprenden de sus equivocaciones debido a que de una forma didáctica se explica la respuesta a la pregunta planteada.

Para un total de 78 personas, y teniendo en cuenta la tabla anterior, las respuestas se distribuyen de acuerdo al gráfico 1. Distribución de puntajes de los participantes en la prueba.

Gráfico 1. Distribución puntajes de los participantes en la prueba.



Fuente: Elaboración propia.

Del gráfico 1. Distribución de puntajes de los participantes en la prueba, se puede observar que para los puntajes de mayor acierto los cuales están entre 265 y 300, el total de personas es de 40, es decir, un poco más de la mitad de la muestra obtuvo resultados asertivos en el uso de la aplicación mientras que, únicamente 10 personas realizaron registro en la aplicación y no contestaron las preguntas.

8. CONCLUSIONES

- La herramienta web diseñada, implementada y probada en ámbitos de sensibilización de usuarios finales en temáticas relacionadas con Seguridad de la Información presenta un ámbito interactivo y brinda a las personas ejemplos de casos reales, buenas prácticas y políticas generales las cuales se presentan como un desafío a manera de concurso, al igual que de una manera divertida, se convierte en un complemento eficaz para que los conceptos de seguridad sean asimilados, generen compromiso y responsabilidad respecto tema la seguridad de la información además de convertirse en un generador de buenas prácticas tanto para el entorno laboral como para el personal.

- Se logró el desarrollo e implementación de una herramienta web que permite apoyar el proceso de sensibilización y cultura en seguridad de la información de las personas, brindando la posibilidad además de tener una visibilidad de las brechas de seguridad asociadas al nivel de conocimiento en seguridad de la información de las personas, permitiendo así enfocar los esfuerzos en los grupos donde se considere que los conocimientos no son os mínimamente requeridos.

- La herramienta y la metodología planteada ayuda a concientizar a las personas en materia de la Seguridad de la Información, aportando de sobremanera a ese reto para todas las organizaciones y para la sociedad en general.

- Durante el diseño y el desarrollo del prototipo se logró que la herramienta adquiera características de enseñanza metodológica, mediante la utilización del juego como motivación para el aprendizaje, con lo cual se pretende mejorar la asimilación de conceptos básicos en torno a la seguridad de la información.

La prueba de campo realizada con la aplicación ratifica el cumplimiento de los objetivos, esto teniendo en cuenta la participación de los servidores públicos, los puntajes y las temáticas tratadas, es así, como la aplicación se torna en un soporte eficaz para las campañas de sensibilización.

RECOMENDACIONES

- Para el uso de la aplicación web en una campaña de sensibilización, es importante acordar previamente la cantidad de preguntas, la cual puede ser extendida o reducida de acuerdo a las necesidades expresadas por las partes interesadas, así mismo, es recomendable personalizar, si es necesario, las preguntas para que estas puedan estar ser alienadas con los objetivos de cada organización.

- Es recomendable adaptar la herramienta de acuerdo a las necesidades específicas de cada organización incluyendo: Logo de organización, cantidad de personas que tendrán acceso a la herramienta, fondo de pantalla, tipo y color de letra, cantidad y contenido de las preguntas, niveles de acceso a categorías de preguntas, ya que esto genera confianza en el uso de la aplicación y sentido de pertenencia y apropiación de la actividad y resultados en el personal de la organización.

- El uso de la herramienta puede ser incentivado por medio de una estímulo a quienes han participado de manera activa en la solución de las preguntas, dicho estímulo estará sujeto a la decisión y consideraciones de cada organización, esto impulsa al personal a una participación activa y motiva el sentido competitivo durante el uso de la aplicación.

BIBLIOGRAFÍA

DELGADO, Andrea, GONZÁLEZ Laura, PIEDRABUENA Federico. Desarrollo de aplicaciones con enfoque SOA (Service Oriented Architecture), Instituto de Computación – Facultad de Ingeniería Universidad de la República Montevideo, Uruguay, 2006.
[Citado el 12 de Marzo de 2016] Disponible en
https://www.colibri.udelar.edu.uy/bitstream/123456789/3528/1/TR0616.pdf

FISMA. Construcción de una Seguridad de la Información, Tecnología de sensibilización y formación, 2002.
[Citado el 12 de Marzo de 2016] Disponible en
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de seguridad de la información para la Estrategia de Gobierno en Línea 2.0, República de Colombia, 2011.
[Citado el 12 de Marzo de 2016] Disponible en
http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

INTERNATIONAL STANDARD ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary, Third edition, 2014.

MINISTERIO DE COMUNICACIONES REPÚBLICA DE COLOMBIA. Capacitación - Modelo de seguridad de la información para la estrategia de Gobierno en Línea, 2008, pp 7.

NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, 2009.

NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la Información (SGSI). Requisitos, 2013.

NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27002. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la seguridad de la Información, 2007.

PORTAFOLIO. Seguridad Informática Certicámara S.A.
[Citado el 02 de Abril de 2016] Disponible en
http://blogs.portafolio.co/seguridad-informatica-certicamara-sa/proteccion-de-datos-personales-una-cultura-de-seguridad/

PORTAFOLIO. Pérdidas delitos informáticos
[Citado el 02 de Abril de 2016] Disponible en
http://www.portafolio.co/economia/finanzas/perdidas-delitos-informaticos-suman-us-93-000-millones-91548

ROMERO, Hairol y ROJAS, Elvin. La Gaminificación como participante del B-Learning: Su percepción en la Universidad Nacional, sede Regional Brunca, Costa Rica. 2013

ROLLINGS, Andrew y MORRIS, Dave. Game Design Architecture, Primera Edición, New Rides, Indianapolis, Estados Unidos, 2003, p. 203

SAVEDRA, O. Guía estratégica para aumentar la efectividad de las campañas de sensibilización de seguridad de la información, Revista Digital Apuntes de Investigación, Bucaramanga, Colombia, Vol 3, Septiembre 2012.
[Citado el 27 de Febrero de 2016] Disponible en
Disponible en: http://apuntesdeinvestigacion.upbbga.edu.co/

VALERA MARISCAL Juan J. F. Gamificación en la Empresa. Madrid: Editorial Círculo Rojo, 2013. Pág 30